Приложение № 1

УТВЕРЖДЕНА
приказом ООО «СК «Ренессанс Жизнь»
от 11.01.2024 № 240111-02-од

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ООО «СК «РЕНЕССАНС ЖИЗНЬ»

Москва – 2024

Руководство ООО «Страховая компания «Ренессанс Жизнь» (далее – Компания), осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности в контексте изменения законодательства и норм регулирования деятельности по защите информации, включая персональные данные, а также в контексте ожиданий клиентов Компании.

Соблюдение требований по информационной безопасности, а также обеспечение конфиденциальности персональных данных клиентов позволит создать конкурентные преимущества Компании, обеспечить ее стабильность, соответствие правовым, регуляторным и договорным требованиям и повышение имиджа.

Информационная безопасность Компании строится в соответствии с законодательством Российской Федерации, нормативными актами и стандартами Банка России, нормативно-методическими документами в области защиты информации Федеральной службы по техническому и экспортному контролю России и Федеральной службы безопасности России, международными и национальными стандартами в области информационной безопасности, документами Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

1. Управление информационной безопасностью в деятельности Компании

1.1. Информационная безопасности (далее - ИБ) – это набор процедур и инструментов, которые обеспечивают в информационной среде всестороннюю защиту конфиденциальной корпоративной информации Компании от неправильного использования, несанкционированного доступа, искажения или уничтожения.

1.2. Процессы по обеспечению ИБ составляют один из видов вспомогательных процессов, реализующих поддержку (обеспечение) процессов основной деятельности Компании.

1.3. Управление ИБ является процессом деятельности Компании, который направлен на содействие в достижении целей деятельности Компании через обеспечение защищенности совокупной информации Компании.

2. Область действия

2.1. Настоящая Политика относится ко всем подразделениям Компании, ко всей информации в любой форме и на любых носителях, к аппаратным средствам и программному обеспечению (далее - ПО), охватывая текущую или будущую деятельность и взаимоотношения с работниками подразделений Компании, ее поставщиками и клиентами.

2.2. Политика охватывает все процессы обработки информации, а также аппаратные средства, ПО, являющиеся средствами обеспечения бизнес-процессов и находящиеся в зоне ответственности Компании.

3. Цели и задачи обеспечения ИБ

3.1. Цели обеспечения ИБ

3.1.1. Информация является активом Компании и должна соответствующим образом оцениваться и защищаться от любых форм несанкционированного доступа, незаконного использования, раскрытия, модификации, разрушения или отказа.

3.1.2. Стратегическими направлениями обеспечения ИБ в Компании, являются:

– устойчивое функционирование и развитие Компании, обеспечение непрерывности предоставления услуг клиентам;
– поддержание статуса Компании как надежного поставщика услуг в области страхования жизни в глазах действующих и потенциальных клиентов, увеличение инвестиционной привлекательности;
– гарантия защищенности процессов и активов, принадлежащих Компании и её клиентам;
– соблюдение законодательных и иных регуляторных требований в области ИБ и защиты персональных данных во всех юрисдикциях, где представлена деятельность Компании.

3.2. **Задачи обеспечения ИБ**

– обеспечение выполнения требований законодательства в области защиты информации и персональных данных, включая требования национальных стандартов и регулирующих документов в области ИБ;

– управление рисками ИБ;

– применение различных организационных и технических мер по обеспечению ИБ, использование передовых технологий противодействия угрозам ИБ;

– вовлечение работников Компании в процессы обеспечения ИБ, повышение уровня ответственности, осведомленности, постоянное обучение и получение обратной связи;

– обеспечение непрерывности бизнеса на основе комплекса организационно-методических и технических мероприятий, направленных на минимизацию последствий утраты информационных активов, а также направленных на бесперебойное оказание услуг клиентам;

– регулярный аудит эффективности процессов, направленных на обеспечение ИБ, анализа со стороны руководства Компании.

4. Описание основных типов защищаемых объектов

К основным защищаемым ресурсам Компании относятся объекты, информационные активы и элементы информационной инфраструктуры, находящиеся в зоне ответственности Компании, в т.ч.:

– информация (данные) автоматизированных, информационных, аналитических систем;

– управляющая информация автоматизированных систем, поддерживающих информационные технологические процессы, информационных систем, поддерживающих технологические процессы, в рамках которых обрабатываются персональные данные (далее - ПДн);

– телекоммуникационная система информационной инфраструктуры Компании;

– технологические процессы;

– программно–технические комплексы (серверная часть, системы хранения данных, сети передачи данных, сетевое и каналообразующее оборудование, каналы связи, рабочие станции) и ПО (прикладное, системное), обеспечивающие реализацию функций как Компании в целом, так и поддержание работы информационной инфраструктуры;

– документация внутреннего делопроизводства;

– документация на программно-аппаратные средства и системы, разработанные (закупленные) по заказу Компании;

– работники Компании, участвующие в обработке информации.

5. Основные средства и меры противодействия потенциальным угрозам

5.1. Защита информационных активов и информационных технологий Компании от потенциальных угроз должна осуществляться комплексным применением следующих мер и средств:

– организационные;

– технологические;

– программные;

– технические.

5.1.1. Для защиты на физическом уровне должны использоваться:

– организационные меры: регламентирование действий персонала; ограничение доступа к оборудованию и носителям информации; внутриобъектовый режим; выбор поставщика, обеспечивающего поставку качественного оборудования и эффективное гарантийное обслуживание; поддержание в актуальном состоянии эксплуатационной документации;

– технологические меры: проведение технического обслуживания; резервирование;

– технические меры: оборудование серверных помещений системами кондиционирования, надежными дверями и механическими замками; оснащение помещений системами контроля доступа, охранно-пожарной сигнализации, средствами пожаротушения; использование систем видеонаблюдения; поддержание в исправном состоянии систем водо- и теплоснабжения; резервирование источников электропитания.

5.1.2. Для защиты на сетевом уровне и уровне сетевых приложений и сервисов должны применяться:

– организационные меры: регламентирование действий персонала; разграничение полномочий и доступа к ресурсам; регламентирование изготовления, хранения и использования паролей и идентификаторов; регламентирование состава ПО; поддержание в актуальном состоянии эксплуатационной документации;

– технологические меры: документирование настроек; создание архивных копий; тестирование ПО; аудит ИБ;

– программные меры: антивирусные средства и программы контроля целостности; блокирование неиспользуемых портов и сервисов; средства аутентификации;

– технические меры: средства межсетевого экранирования; средства защиты от несанкционированного доступа.

5.1.3. Защита на уровне операционных систем должна включать:

– организационные меры: регламентирование администрирования; регламентирование установки и обновления ПО, в том числе непосредственно операционных систем; разграничение полномочий и доступа к ресурсам; порядок формирования и смены паролей; регламентирование конфигурации и состава ПО; регламентирование антивирусного контроля;

– технологические меры: создание архивных копий; тестирование ПО; антивирусный контроль; аудит ИБ;

– программные меры: антивирусное ПО; средства контроля целостности; средства аутентификации; средства обнаружения и предотвращения вторжений, средства анализа защищенности;

– технические меры: средства защиты от НСД.

5.1.4. Для защиты на уровне систем управления базами данных должны быть применены:

– организационные меры: регламентирование администрирования; разграничение полномочий и доступа к ресурсам; порядок формирования и смены паролей; обеспечение достаточного уровня квалификации администратора; документирование технологических процессов администрирования; регламентирование обновления ПО;

– технологические меры: создание архивных копий баз данных; ведение баз данных «горячего резерва»; хранение эталонных копий ПО СУБД; аудит ИБ;

– программные меры: средства аутентификации; средства шифрования при необходимости; средства контроля целостности объектов баз данных.

5.1.5. На уровне производственных процессов и приложений должны использоваться:

– организационные меры: регламентирование действий исполнителя; регламентирование внесения изменений в технологию; регламентирование состава прикладного ПО; порядок формирования ролей и полномочий персонала; регламентирование формирования, хранения и смены паролей, ключевой информации, атрибутов доступа; регламентирование сопровождения приложения (задачи); отделение от средств разработки;

– технологические меры: выполнение контрольных операций (повторный ввод), документирование процесса; мониторинг контрольных точек процесса; организация независимых контуров контроля;

– программные меры: средства ЭП (коды аутентификации), средства шифрования при необходимости, средства регистрации действий пользователя, средства контроля целостности приложений.

5.1.6. Для защиты на уровне бизнес-процессов Компании должны использоваться в основном организационные меры, заключающиеся в подборе персонала, назначении и распределении ролей, соответствующих задачам Компании, установлении персональной ответственности за их исполнение. А также документирование самих бизнес-процессов и своевременное обновление такой документации.

6. Принципы управления информационной безопасностью

Компания в области информационной безопасности руководствуется следующими основными принципами:

– Законность. Защита активов Компании соответствует положениям и требованиям действующего законодательства.

– Системность. Системный подход к обеспечению требований информационной безопасности означает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения задачи защиты информации.

– Комплексность. Информационная безопасность обеспечивается эффективным сочетанием организационных, методических мер и программно-технических средств. Применение различных средств и технологий защиты процессов и активов снижает вероятность реализации наиболее значимых угроз информационной безопасности.

– Непрерывность совершенствования. Меры и средства защиты активов постоянно совершенствуются, учитывается появление новых способов и средств реализации угроз информационной безопасности, а также принимается во внимание имеющийся опыт других организаций в сфере информационной безопасности.

– Разумная достаточность и адекватность. Программно-технические средства и организационные меры, направленные на защиту активов, проектируются и внедряются на основе регулярной оценки рисков таким образом, чтобы не повлечь за собой существенное ухудшение основных функциональных характеристик, а также производительности информационных систем Компании.

– Персональная ответственность. Ответственность за обеспечение безопасности активов возлагается на каждого работника в пределах его полномочий.

– Контроль. Оценка эффективности системы защиты информации является неотъемлемой частью работ по обеспечению информационной безопасности. С целью своевременного выявления и пресечения попыток нарушения установленных правил обеспечения безопасности активов, в Компании определены процедуры постоянного контроля использования систем обработки и защиты активов, а результаты контроля подвергаются регулярному анализу.

7. Основные требования по обеспечению ИБ

7.1. В целях реализации настоящей Политики, в Компании функционирует Служба ИБ, занимающаяся направлением информационной безопасности, с отдельной статьей бюджета для финансирования обеспечения ИБ.

7.2. Владельцем внутренних нормативных документов по информационной безопасности является Служба ИБ. Любые вопросы по интерпретации указанных документов должны быть адресованы в Службу ИБ. Перечень документов приведен в приложении № 1 настоящей Политики.

7.3. Любые процессы, продукты и процедуры, касающиеся информационных систем и информации Компании (например, описан цикл обработки и хранения определенной информации в любой форме), а также связанные с ИБ и определенные в Политике и Стандартах ИБ, должны быть согласованны со Службой ИБ.

7.4. Служба ИБ участвует в качестве согласующего подразделения в любых проектах/активности компании в рамках которых вносятся изменения в существующие или создаются новые информационные системы/ресурсы/активы.

7.5. Служба ИБ самостоятельно определяет степень своего участия в таких проектах основываясь на требованиях законодательства Российской Федерации, стандартах и предписаниях Банка России, лучших мировых практиках, а также собственном экспертном опыте.

Служба ИБ несет ответственность за реализацию настоящей Политики, а также за соответствие положений Политики информационной безопасности требованиям действующего законодательства Российской Федерации, доведение и разъяснение их работникам Компании и заинтересованным сторонам, назначение ответственных за решение соответствующих задач для достижения этих целей на всех уровнях, а также за их реализацию, периодический анализ и пересмотр. Положения настоящей Политики информационной безопасности являются обязательными для исполнения работниками всех структурных подразделений Компании.

Приложение № 1 к Политике информационной безопасности ООО «СК «Ренессанс Жизнь», утвержденной приказом от 11.01.2024 № 240111-02-од

Перечень утвержденных документов, регламентирующих ИБ

Перечень документов, регламентирующих ИБ в компании включает, но не ограничивается следующие документы:

- Область применения процессов системы защиты информации;
- Положение о внутренних проверках информационной безопасности;
- Положение о работе с мобильными устройствами;
- Положение по антивирусной защите;
- Положение по безопасной разработке;
- Положение по защите виртуальной инфраструктуры;
- Положение по обеспечению ИБ на стадиях жизненного цикла автоматизированных систем;
- Положение по обеспечению сетевой безопасности;
- Положение по обучению и повышению осведомленности в области ИБ;
- Регламент по работе с машинными носителями информации;
- Регламент управления доступом к информационным ресурсам;
- Регламент актуализации доступа к информационным активам;
- Регламент управления уязвимостями;
- Порядок совершенствования системы обеспечения информационной безопасности;
- Регламент реагирования на инциденты ИБ;
- Положение о работе с корпоративной электронной почтой;
- Положение о защите коммерческой тайны;
- Инструкции пользователя по обеспечению информационной безопасности;
- Модель угроз и нарушителя безопасности информации, обрабатываемой на объектах критической информационной инфраструктуры;
- Политика в области обработки персональных данных;
- Положение по организации обработки персональных данных;
- Регламент обеспечения безопасности персональных данных;
- Регламент взаимодействия с субъектами персональных данных;
- Цели обработки персональных данных;
- Инструкция пользователя по правилам обработки и обеспечения безопасности персональных данных;
- Описание информационных систем персональных данных;
- Перечень персональных данных;
- Модели угроз безопасности информации при ее обработке в информационных системах персональных данных (13 отдельных документов в соответствии с количеством информационных систем персональных данных);
- Положение о внутриобъектовом режиме;
- Регламент предоставления ИТ-сервисов;
- Регламент резервного копирования;
- Парольная политика.