Утверждено
решением Совета директоров
АО «СК «Сентрас Иншуранс»
Протокол № 35 от 30 мая 2022 г.

Согласовано
решением Правления
АО «СК «Сентрас Иншуранс»
Протокол № 27 от 30 мая 2022 г.

П-08

Политика информационной безопасности

Контроль	Комплаенс-контролер	Бимагамбетова А.С.	27.05.2022	
			(дата)	(подпись)

Должность, подразделение	ФИО	Виза	Дата	Подпись
Директор ТД	Кулназаров Г.Ж.	Согласовано по СЗ № ВНД-17-16-22/14	27.05.2022	
Риск-менеджер	Башпанов У.Д.		27/05/2022	
Начальник УПО ЮД	Байназарова А.Х.		27.05.2022	
Заместитель Директора ТД	Койлыбаева А.Н.		27.05.2022	

Разработал	Начальник Службы информационной безопасности	Дулатов К.О.	27.05.2022	
			(дата)	(подпись)

Содержание

1. Общие положения и область применения

1. Настоящая Политика информационной безопасности (далее - Политика) определяет общие направления, основные цели и задачи по обеспечению защиты информации, действия АО «СК «Сентрас Иншуранс» (далее - Общество) по обеспечению эффективной информационной защиты.

2. Осуществление основной деятельности Общества тесно связано с обработкой и хранением информации и обеспечением сохранности и защиты информации от несанкционированного доступа к данным, а также кибербезопасности.

3. Для организации безопасной работы в Обществе внедряется система управления информационной безопасностью, являющаяся частью общей системы управления Обществом и предназначенная для управления процессом обеспечения информационной безопасностью.

4. Политика включает описание состава применяемых информационных систем, списка пользователей, их права на доступ к информации, программным и техническим средствам согласно Приложению №1 к Политике и устанавливает совокупность принципов и следующих требований в области информационной безопасности:

1) по организации доступа к создаваемой, хранимой и обрабатываемой информации в информационных системах Общества, мониторинга информации и доступа к ней;

2) по осуществлению сбора, консолидации и хранения информации об инцидентах информационной безопасности;

3) по мониторингу деятельности по обеспечению информационной безопасности;

4) к проведению анализа информации об инцидентах информационной безопасности;

5) по ответственности работников за обеспечение информационной безопасности при исполнении возложенных на них функциональных обязанностей.

5. Политика разработана в соответствии с Законом Республики Казахстан «О страховой деятельности» от 18 декабря 2000 года №126-II, Правилами формирования системы управления рисками и внутреннего контроля страховых (перестраховочных) организаций, утвержденными Постановлением Правления Национального Банка Республики Казахстан от 27 августа 2018 года №198, 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 и Требованиями к деятельности организации по формированию и ведению базы данных, утвержденными Постановлением Правления Национального Банка Республики Казахстан от 25 июня 2007 года №177, Требованиями к программно-техническим средствам и интернет-ресурсам страховой (перестраховочной) организации, филиала страховой (перестраховочной) организации-нерезидента Республики Казахстан, обеспечивающим заключение договоров страхования, обмен электронными информационными ресурсами между страхователем и страховщиком, утвержденными постановлением Правления Агентства Республики Казахстан по регулированию и развитию финансового рынка от 27 апреля 2020 года № 50.

6. Положения Политики обязательны к исполнению всеми работниками Общества.

7. Требования Политики распространяются на всю информацию и ресурсы обработки информации Общества.

2. Определения, термины, сокращения

8. В Политике используются следующие понятия и сокращения:

1) **DDoS-атака** - распределенная атака типа «отказ в обслуживании» со стороны третьих лиц с целью нарушения штатного режима работы информационной системы или создание условий, при которых свободный доступ к предоставляемым информационным ресурсам будет недоступен либо затруднен;

2) **анти-бот** - тест или программное обеспечение, с использованием которого запрашивается подтверждение того, что к интернет-ресурсу обращается человек, а не бот;

3) **атака** - попытка уничтожения, раскрытия, изменения, ограничения доступа, кражи, получения несанкционированного доступа или несанкционированного использования информационного актива;

4) **бот** - программное обеспечение, используемое третьими лицами для автоматического выполнения определенных операций по заданному расписанию и (или) алгоритму в информационной системе Общества;

5) **доступ** - возможность использования информационных активов;

6) **информационная безопасность** - состояние защищенности электронных информационных ресурсов, информационных систем и информационной инфраструктуры от внешних и внутренних угроз;

7) **информационная система (ИС)** - информационная система, в которой хранятся и обрабатываются данные Общества и ее клиентов;

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

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

10) **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;

11) **обеспечение информационной безопасности** - процесс, направленный на поддержание состояния конфиденциальности, целостности и доступности информационных активов Общества;

12) **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;

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

14) **РК** - Республика Казахстан;

15) **СУБД** - система управления базами данных;

16) **СУИБ** - система управления информационной безопасностью;

17) **угроза информационной безопасности** - совокупность условий и факторов, создающих предпосылки к возникновению инцидента информационной безопасности;

18) **уполномоченный орган** - Агентство по регулированию и развитию финансового рынка;

19) **центр обработки данных** - специально выделенное помещение, в котором размещено серверное и коммуникационное оборудование информационной инфраструктуры Общества.

3. Цели, задачи и основные принципы построения СУИБ

9. Целями построения СУИБ являются:

1) обеспечение защиты информационных активов;

2) обеспечение информационной безопасности.

10. Общество обеспечивает функционирование СУИБ, ее развитие и улучшение.

11. Реализация целей СУИБ достигается путем решения следующих основных задач:

1) формирование внутренней организационной структуры СУИБ посредством распределения должностных обязанностей, сфер ответственности и полномочий;

2) контроль доступа к информационным активам, информационным системам;

3) обеспечение непрерывности функционирования информационной инфраструктуры;

4) противодействие угрозам и работа с инцидентами информационной безопасности;

5) обеспечение физической безопасности;

6) определение вопросов информационной безопасности, связанных с персоналом и повышение осведомленности в области информационной безопасности.

12. Формирование СУИБ Общества и ее функционирование осуществляются в соответствии со следующими основными принципами:

1) **законность** - любые действия, предпринимаемые для обеспечения информационной безопасности, осуществляются на основе действующего законодательства РК;

2) **ориентированность на бизнес** - информационная безопасность рассматривается как процесс поддержки основной деятельности Общества. Мероприятия по обеспечению информационной безопасности не должны повлечь за собой серьезных препятствий деятельности Общества;

3) **экономическая целесообразность** - стоимость защитных мер и систем по поддержанию информационной безопасности не должна превышать размера возможного ущерба;

4) **минимизация привилегий** - предоставление минимальных прав доступа;

5) **приоритетность** - категорирование информационных активов по степени важности;

6) **информированность и персональная ответственность** - работники Общества обязаны знать требования информационной безопасности Общества и несут персональную ответственность за выполнение этих требований;

7) **взаимодействие и координация** - обеспечение информационной безопасности осуществляются на основе взаимосвязи и координации соответствующих структурных подразделений Общества.

4. Требования по организации информационной безопасности

13. В целях построения и развития СУИБ, в Обществе определяются требования к организации доступа к создаваемой, хранимой и обрабатываемой информации в используемых Обществом информационных системах, мониторингу информации и доступу к ней, включая:

1) предоставление доступа через систему заявок, идентификация подключаемых к информационным системам пользователей и разграничение доступа пользователям информационных систем на основании норм, установленных соответствующими внутренними документами Общества: «И-02 Порядок пользования ресурсами локальной вычислительной сети», «И-31 Матрица доступов КИАС»;

2) мониторинг сетевого трафика, событий антивирусного программного обеспечения и событий безопасности системного и прикладного программного обеспечения с применением норм, установленных внутренним нормативным документом Общества «И-03 Процедура по предотвращению утечки конфиденциальной информации и искажению информационных данных»;

3) сбор и консолидация информации при выявлении инцидентов информационной безопасности, проведение анализа информации об инцидентах информационной безопасности в целях планирования превентивных мер защиты и улучшения процесса обеспечения информационной безопасности в целом, хранение информации об инциденте информационной

безопасности в соответствии с внутренними нормативными документами Общества: «И-32 Порядок обработки инцидентов информационной безопасности», «И-33 Порядок обеспечения физической безопасности информационных активов»;

4) обеспечение антивирусной защиты информационной инфраструктуры согласно внутреннего нормативного документа «И-03 Процедура по предотвращению утечки конфиденциальной информации и искажению информационных данных»;

5) осуществление резервного хранения данных информационных систем, их файлов и настроек, обеспечивающих восстановление работоспособных копий информационных систем на основании внутреннего нормативного документа «И-04 Инструкция о резервном копировании информации»;

6) обеспечение физической безопасности центра обработки данных с применением норм внутреннего нормативного документа Общества «И-33 Порядок обеспечения физической безопасности информационных активов»;

7) контроль обновления информационных систем Общества и определение порядка управления обновлениями «И-03 Процедура по предотвращению утечки конфиденциальной информации и искажению информационных данных»;

8) реализация действий, предотвращающих 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 согласно норм, установленных внутренним нормативным документом Общества «П-21 План на случай чрезвычайных обстоятельств и обеспечения непрерывности деятельности АО «СК «Сентрас Иншуранс»;

9) недопущение использования неуполномоченными работниками Общества учетных записей (криптографических ключей, ключей электронной цифровой подписи) для несанкционированного доступа в ЕСБД с использованием технических и технологических методов защиты согласно норм, установленных внутренним нормативным документом «И-28 Инструкция по работе в Единой страховой базе данных».

14. В рамках требований к программно-техническим средствам и интернет-ресурсам, Общество обеспечивает защиту своего интернет-ресурса и информационных систем от ботов, DDoS-атак и применения иного зловредного программного обеспечения со стороны третьих лиц путем использования анти-бот решений и иных технических и технологических методов защиты.

5. Разделение полномочий и ответственности

15. Система информационной безопасности напрямую зависит от заинтересованности всех работников Общества.

16. В Обществе участниками СУИБ являются:

1) Совет директоров;

2) Правление;

3) Служба информационной безопасности и ответственное лицо по вопросам физической и технической безопасности (работник Административного управления);

4) Департамент программирования;

5) Комплаенс-контролер;

6) Служба внутреннего аудита;

7) Юридический департамент;

8) HR-Департамент.

17. Совет директоров Общества:

1) утверждает настоящую Политику и Перечень защищаемой информации, включающий информацию о сведениях, составляющих тайну страхования, служебную, коммерческую или иную охраняемую законом тайну, и порядок работы с защищаемой информацией;

2) принимает ответственность по утверждению и контролю за исполнением ответственными структурными подразделениями требований, установленных Политикой;

3) проводит контроль за состоянием СУИБ.

18. Правление Общества в целях функционировании СУИБ:

1) обеспечивает независимость Службы информационной безопасности от подразделений по информационным технологиям (Департамента программирования, Управления системного администрирования), посредством их подчинения разным членам Правления или напрямую Председателю Общества;

2) принимает решения о балансе между затратами на реализацию средств контроля и бюджетными отчислениями;

3) утверждает внутренние документы, регламентирующие процесс обеспечения информационной безопасности, порядок и периодичность пересмотра которых определяется внутренними документами.

19. Служба информационной безопасности в целях обеспечения конфиденциальности, целостности и доступности информации Общества осуществляет следующие функции:

1) организует СУИБ, осуществляет координацию и контроль деятельности подразделений Общества по обеспечению информационной безопасности и мероприятий по выявлению и анализу угроз, противодействию атакам и расследованию инцидентов информационной безопасности;

2) разрабатывает Политику информационной безопасности;

3) обеспечивает поддержку систем защиты и методологическую поддержку процесса обеспечения информационной безопасности;

4) осуществляет выбор, внедрение и применение методов, средств и механизмов управления, обеспечения и контроля информационной безопасности в рамках своих полномочий;

5) осуществляет сбор, консолидацию, хранение и обработку информации об инцидентах информационной безопасности;

6) осуществляет анализ информации об инцидентах информационной безопасности;

7) организует и проводит мероприятия по обеспечению осведомленности работников Общества в вопросах информационной безопасности;

8) осуществляет мониторинг состояния СУИБ;

9) осуществляет информирование руководства Общества о состоянии СУИБ;

10) не позднее 10 (десятого) января года, следующего за отчетным годом, представляет в Уполномоченный орган информацию о состоянии СУИБ в электронном формате с использованием транспортной системы гарантированной доставки информации с криптографическими средствами защиты, обеспечивающей конфиденциальность и некорректируемость представляемых данных. Информация о состоянии СУИБ должна включать следующие сведения о:

a) наличии документов, регламентирующих создание и функционирование СУИБ;

b) наличии и количественном составе программно-технических средств, используемых для обеспечения информационной безопасности;

c) наличии, материально-технической обеспеченности центров обработки данных;

d) проведенных мероприятиях по совершенствованию СУИБ и информационных активов Общества либо их отсутствии.

20. Департамент программирования совместно с Управлением системного администрирования осуществляет следующие функции:

1) поддерживает прикладное программное обеспечение и работоспособность информационных систем и системы их защиты;

2) разрабатывает схемы информационной инфраструктуры Общества;

3) обеспечивает предоставление доступа работникам к информационным активам;

4) обеспечивает исполнение установленных требований по непрерывности функционирования информационной инфраструктуры, конфиденциальности, целостности и доступности информационных систем Общества (включая резервирование и (или) архивирование) в соответствии с нормами внутренних нормативных документов;

5) соблюдает исполнение внутренних документов Общества, содержащих требования к информационной безопасности при выборе, внедрении, разработке и тестировании информационных систем;

6) отслеживает обновления информационных систем Общества и совместно со Службой информационной безопасности определяют порядок управления обновлениями информационных систем.

21. Ответственное лицо за обеспечение физической и технической безопасности Общества (работник Административного управления):

1) осуществляет меры физической и технической безопасности, в том числе организует пропускной и внутриобъектовый режим;

2) проводит профилактические мероприятия, направленные на минимизацию рисков возникновения угроз информационной безопасности при приеме на работу и увольнении работников Общества.

22. HR-Департамент осуществляет следующие функции:

1) обеспечивает подписание работниками, а также лицами, привлеченными к работе по договору об оказании услуг, стажерами, практикантами обязательств о неразглашении конфиденциальной информации;

2) участвует в организации процесса повышения осведомленности работников в области информационной безопасности.

23. Юридический департамент осуществляет правовую экспертизу внутренних документов Общества по вопросам обеспечения информационной безопасности.

24. Служба внутреннего аудита проводит оценку адекватности и эффективности контроля за рисками информационных систем Общества и состояния СУИБ в соответствии с внутренними документами, регламентирующими организацию системы внутреннего аудита Общества.

25. Комплаенс-контролер совместно с Юридическим департаментом определяет виды информации, подлежащие включению в перечень защищаемой информации, утвержденный Советом директоров.

26. Руководители структурных подразделений Общества:

1) обеспечивают ознакомление работников с требованиями к информационной безопасности;

2) несут персональную ответственность за обеспечение информационной безопасности в возглавляемых ими подразделениях.

27. Работники структурных подразделений Общества:

1) обеспечивают соблюдение требований к информационной безопасности, принятых в Обществе;

2) извещают своего непосредственного руководителя и Службу информационной безопасности обо всех подозрительных ситуациях и нарушениях при работе с информационными активами.

28. Работники и другие лица, с которыми Общество заключает договоры об оказании услуг, несут ответственность за безусловное и безоговорочное исполнение своих обязанностей по поддержке деятельности обеспечения и выполнения требований информационной безопасности в соответствии с документами системы информационной безопасности, размещенными в общедоступном ресурсе Общества.

29. Лица, являющиеся при договорных отношениях, третьей стороной и имеющие доступ к информационным системам Общества, несут ответственность в соответствии с договорными обязательствами.

6. Заключительные Положения

30. Информация об инцидентах информационной безопасности, полученная в ходе мониторинга деятельности по обеспечению информационной безопасности, подлежит консолидации, систематизации и хранению не менее 5 (пяти) лет.

31. Политика подлежит пересмотру Службой информационной безопасности и технологическим Департаментом:

1) по итогам внутреннего анализа актуальности определенных в ней положений, но не реже 1 (одного) раза в 3 (три) года;

2) в случае существенных изменений в бизнес-процессах Общества, а также требований законодательства РК или уполномоченного органа.

7. Приложения

Приложение №1 - «Состав применяемых информационных систем Общества, список пользователей, их права на доступ к информации, программным и техническим средствам».

Приложение №1 к «П-08 Политика информационной безопасности»

Состав применяемых информационных систем Общества, список пользователей, их права на доступ к информации, программным и техническим средствам

1. Состав ИС КИАС:

1) Сервер баз данных - основной сервер, осуществляющий хранение данных. Используемое программное обеспечение: СУБД Oracle 12c.;

2) сервер web-приложений - сервисы web интеграции и web приложений. Используемое программное обеспечение: Internet Information Services (IIS) for Windows;

3) файл - сервер - хранилище документов, прикрепляемых в ИС;

4) адаптеры КИАС - приложения для интеграции ИС с различными внешними системами.

2. Список пользователей ИС КИАС, их права доступа:

1) Список меню «Настройка КИАС» - «Пользователи КИАС»;

2) Доступ к ИС осуществляется путем идентификации и аутентификации пользователей информационных систем. Порядок разграничения и предоставления прав доступа регламентирован во внутреннем документе «И-31 Матрица доступов КИАС».

3. Состав ИС 1С 8.3:

1) Сервер баз данных - хранилище данных. Используемое программное обеспечение: СУБД MSSQL Server.

2) Сервер администрирования 1С - сервис обеспечения клиент-серверного варианта работы системы 1С.

4. Список пользователей ИС 1С 8.3, их права доступа:

1) Меню «Администрирование» - «Пользователи» (Конфигуратор);

2) Порядок разграничения и предоставления прав доступа регламентирован соответствующим внутренним документом.