ООО «Облачные технологии» +7 (495) 260-10-82
Cloud technology Limited (Ltd.) www.sbercloud.ru

УТВЕРЖДЕНА
приказом ООО «Облачные технологии»
от «24» сентября 2021 г. № П-8.512

ПОЛИТИКА КИБЕРБЕЗОПАСНОСТИ

Оглавление

1. НАЗНАЧЕНИЕ

1.1. Настоящий документ (далее – Политика) определяет политику кибербезопасности в ООО «Облачные технологии» (далее – Компания), как систему документированных управленческих решений, направленных на защиту определенных защищаемых процессов и активов Компании, клиентов и партнеров.

1.2. Настоящая Политика является документом, доступным каждому работнику Компании и представляет собой официально принятую руководством ООО «Облачные технологии» систему взглядов на проблему обеспечения кибербезопасности, и устанавливает принципы построения системы управления информационной безопасностью (далее – СУИБ) на основе систематизированного изложения целей, процессов и процедур кибербезопасности Компании.

1.3. Настоящая Политика Компании может быть предоставлена официальным представителям любых органов и ведомств Российской Федерации, представителям органов сертификационного аудита, клиентам и партнерам Компании, подрядным организациям и частным лицам, выполняющим работы для Компании, а также другим заинтересованным организациям и лицам как на территории Российской Федерации, так и за ее пределами. Политика разработана на русском языке, в соответствии с законодательством Российской Федерации, положениями международных стандартов ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019, документами по управлению рисками, а также с учетом накопленного опыта в сфере обеспечения безопасности информационных технологий в Компании.

1.4. Настоящая Политика разработана с целью установления единого подхода в Компании к управлению безопасностью информации.

1.5. В целях настоящей Политики термин «кибербезопасность» включает в себя в том числе понятие информационной безопасности и безопасности информационных технологий Компании.

2. ОБЛАСТЬ ПРИМЕНЕНИЯ

2.1. Политика обязательна для применения во всех подразделениях и всеми работниками Компании, при обеспечении и управлении кибербезопасностью Компании.

2.2. Положения Политики распространяются на все аспекты деятельности Компании, тем или иным образом влияющие на кибербезопасность активов клиентов, партнеров и самой Компании.

2.3. Действие Политики распространяется на деятельность всех подразделений Компании.

2.4. Требования настоящего документа распространяются на процессы предоставления сервисов в области информационных технологий, включая облачные сервисы, сервисы эксплуатации, технической поддержки, мониторинга и обслуживания сетевой инфраструктуры, вычислительных систем, комплексов и программного обеспечения, предоставляемых внешним и внутренним клиентам, партнерам.

3. ДЕКЛАРАЦИЯ ПРИВЕРЖЕННОСТИ РУКОВОДСТВА КОМПАНИИ

3.1. Руководство Компании осознает важность и необходимость развития и совершенствования мер и средств обеспечения кибербезопасности в контексте развития законодательства и норм регулирования деятельности по защите информации, а также развития защищенных облачных технологий и ожиданий партнеров и других заинтересованных сторон. Соблюдение требований кибербезопасности, а также обеспечение конфиденциальности персональных данных позволит создать конкурентные преимущества Компании, обеспечить её стабильность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

3.2. Руководство Компании обязуется обеспечивать необходимыми ресурсами на поддержку и модернизацию СУИБ в соответствие с требованиями международных стандартов ISO/IEC 27001:2013, ISO/IEC 27017:2015, ISO/IEC 27018:2019 и ISO/IEC 27701:2019.

3.3. На Руководство Компании возлагается ответственность за организацию деятельности по обеспечению кибербезопасности, процесса анализа и оценки пригодности системы защиты информации, ее адекватности, результативности и возможностям улучшения.

3.4. Ответственность за реализацию процессов обеспечению кибербезопасности в Компании возлагается на Руководство Компании, Центр киберзащиты (далее – ЦКЗ) и каждого работника Компании.

3.5. Руководство Компании должно обеспечить мотивацию персонала по обеспечению кибербезопасности Компании.

4. ЦЕЛИ И ЗАДАЧИ

4.1. Общими целями Компании являются:

- развитие информационных и облачных технологий в Российской Федерации;
- расширение количества и улучшение качества оказываемых услуг и сервисов клиентам с одновременным снижением затрат для клиентов и увеличением прибыли Компании за счет применения новых технологий, в том числе облачных сервисов, облачных вычислений и облачного хранения данных;
- поддержание репутации ведущего облачного провайдера в России;
- создание и развитие новых продуктов;
- расширение географии деятельности Компании;
- развитие отношений с российскими и зарубежными партнерами;
- повышение качества управления Компанией посредством использования международных стандартов.

4.2. Целями обеспечения кибербезопасности в Компании являются:

- устойчивое функционирование и развитие Компании, обеспечение непрерывности предоставления услуг клиентам и партнерам;
- поддержание статуса Компании как надежного поставщика облачных услуг в глазах потенциальных клиентов, увеличение инвестиционной привлекательности;
- гарантия защищенности процессов и активов, принадлежащих Компании, её клиентам и партнерам;
- обеспечение постоянного, открытого, прозрачного управления и контроля процессов обеспечения кибербезопасности и защиты персональных данных.

4.3. Защищенность активов Компании, клиентов и партнеров оценивается и обеспечивается по каждому из следующих аспектов:

- доступность;
- целостность;
- конфиденциальность.

4.4. При этом критерием оценки является вероятность, размер и последствия нанесения Компании любого вида ущерба (невыполнение имеющихся перед государством, клиентами и партнерами обязательств, финансовые потери, потеря репутации и пр.).

4.5. Целями внедрения СУИБ в Компании являются:

- получение Руководством прозрачного процесса планирования бюджета ЦКЗ в части обеспечения кибербезопасности на основе риск-ориентированного подхода;
- снижение актуальных рисков кибербезопасности и одновременное выполнение требований законодательства и нормативно-правовых актов Российской Федерации применением типовых наборов средств защиты информации (далее – СЗИ). Это позволит сократить затраты на дублирующие по функционалу СЗИ, их обслуживающий персонал, позволит улучшить производительность систем, для защиты которых применяются СЗИ;
- удешевление внутренних процессов Компании за счет учета вопросов обеспечения кибербезопасности на ранней стадии заключения новых договоров, проектирования новых услуг, автоматизированных систем, а также на старте новых проектов Компании;
- обеспечение процесса расследования инцидентов, связанных с безопасностью информации, сбора доказательной базы для отстаивания интересов Компании, в том числе в суде;
- определение ответственности между подразделениями Компании за обеспечение кибербезопасности.

4.6. Задачами СУИБ Компании являются:

- определение активов, подлежащих защите;
- защита конфиденциальной информации в соответствии с законодательством Российской Федерации, в том числе, но не ограничиваясь: персональных данных, сведений, составляющих коммерческую тайну, информации, полученной при

осуществлении деятельности Компании от клиентов, партнеров и других источников, а также информации, определенной Компанией, как нуждающейся в ограничении распространения;

- обеспечение выполнения требований нормативных правовых актов Российской Федерации в сфере информационной безопасности;
- организация управления рисками, связанными с нарушением безопасности информационных активов Компании, при котором риски постоянно контролируются и исключаются, либо находятся на допустимом (приемлемом) уровне остаточного риска, либо имеется четкий план со сроками по их снижению/передаче;
- 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;
- управление инцидентами, связанными с безопасностью информации, при этом любой факт (инцидент) нарушения требований по информационной безопасности рассматривается как существенное событие и требует разбирательства;
- противодействие новейшим комплексным угрозам кибербезопасности, таким как постоянные угрозы повышенной сложности APT (Advanced Persistent Threat), угрозы нулевого дня (0-day) и т.д.;
- минимизация потерь и скорейшее восстановление инфраструктуры, программных и технических средств, а также информации, вследствие кризисных (нештатных) ситуаций. Расследование причин возникновения таких ситуаций и принятие мер по их предотвращению в будущем;
- регулярная оценка соответствия СУИБ применимым внутренним и внешним требованиям посредством проведения внутренних аудитов, мониторинга эффективности процессов СУИБ, анализа со стороны руководства Компании;
- внедрение корректирующих действий в случае выявления отклонений или несоответствий в работе СУИБ внутренним и внешним требованиям;
- наращивание компетенции ЦКЗ в области кибербезопасности, в целях повышения качества услуг, оказываемых клиентам Компании.

4.7. В результате реализации целей кибербезопасности и, в частности, целей и задач СУИБ в Компании разработан и внедрен комплекс организационно-методических и технических мероприятий.

4.8. Данные мероприятия являются базовой составляющей обеспечения и управления кибербезопасностью в Компании.

5. ПРИНЦИПЫ УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ

5.1. Основные принципы управления кибербезопасностью.

Компания в области кибербезопасности руководствуется следующими основными принципами.

- Законность защиты:

защита активов Компании соответствует положениям и требованиям действующих законов и иных нормативных правовых актов Российской Федерации.

- Системность защиты:

системный подход к обеспечению кибербезопасности означает учёт всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения задачи обеспечения кибербезопасности Компании.

- Комплексность защиты:

кибербезопасность 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 кибербезопасности.

- Непрерывность защиты:

функционирование процессов кибербезопасности на всех этапах работы с активами Компании. В Компании осуществляется постоянный мониторинг и аудит процессов кибербезопасности.

- Своевременность:

означает упреждающий характер принимаемых мер по обеспечению кибербезопасности.

- Гибкость:

предполагает, что в процессе эксплуатации активов Компании изменения характеристик, объёма и категорий обрабатываемой информации влекут за собой своевременные и адекватные изменения в структуре управления кибербезопасности.

- Непрерывность совершенствования:

означает, что меры и средства защиты активов постоянно совершенствуются в соответствии с результатами анализа функционирования структуры кибербезопасности, учитывается появление новых способов и средств реализации угроз кибербезопасности, а также принимается во внимание имеющийся отечественный и зарубежный положительный опыт в сфере кибербезопасности. В процессе непрерывного совершенствования осведомленности работников в части кибербезопасности проводится периодическое обучение.

- Документированность:

документирование обеспечивает закрепление достигнутого текущего состояния обеспечения кибербезопасности. Любые изменения этого состояния оформляются документально.

- Разумная достаточность и адекватность:

принимаемые меры обеспечения кибербезопасности эффективны и соразмерны имеющим место рискам кибербезопасности, связанных с обработкой и характером защищаемых активов, на основании результатов оценки рисков кибербезопасности; программно-технические средства и организационные меры, направленные на защиту активов, проектируются и внедряются таким образом, чтобы не повлечь за собой существенное ухудшение основных функциональных характеристик, а также производительности информационных систем и работников Компании.

- Осведомленность о риске кибербезопасности:

процессы обеспечения кибербезопасности затрагивают каждого работника Компании, использующего ее информационные активы, и накладывают на него соответствующие обязанности и ограничения.

- Персональная ответственность:

означает, что ответственность за обеспечение безопасности активов возлагается на каждого работника в пределах его трудовых обязанностей. Помимо этого, в ЦКЗ назначены ответственные лица за поддержание процессов обеспечения и управления кибербезопасности.

- Минимизация полномочий:

каждому работнику Компании доступ к информационным активам предоставляется только в том объеме, который необходим ему для выполнения трудовых обязанностей. Все операции по предоставлению доступа или назначению полномочий ограничены, контролируются и осуществляются строго в соответствии с установленными процедурами.

- Взаимодействие и сотрудничество:

означает, что в коллективе Компании создана благоприятная атмосфера, способствующая осознанной необходимости соблюдения установленных правил и оказания содействия в деятельности подразделений, обеспечивающих кибербезопасность.

- Разделение полномочий по управлению информационными технологиями:

в Компании реализована структура управления информационными технологиями, направленная на исключение конфликта интересов и строгое разграничение ответственности при обеспечении функционирования и безопасности информационных активов: разделены обязанности подразделений и работников Компании, осуществляющих администрирование коммуникационного оборудования, средств защиты, и осуществляющих функции мониторинга состояния кибербезопасности и контроля (аудита) выполнения требований кибербезопасности.

- Специализация и профессионализм:

означает, что к разработке средств и реализации мер защиты активов привлекаются специализированные организации или работники ЦКЗ, наиболее подготовленные к

конкретному виду деятельности по обеспечению кибербезопасности и имеющие опыт практической работы.
реализация административных мер и эксплуатация средств защиты информации (активов) осуществляется профессионально подготовленными специалистами ЦКЗ.

- Знание своих партнеров и работников:

Компания обладает информацией о своих партнерах, что позволяет минимизировать вероятность реализации угроз, связанных с человеческим фактором;
кадровая политика (подбор персонала, мотивация работников), используемая в Компании, обеспечивает исключение или минимизацию возможностей работников Компании по нарушению системы безопасности активов.

- Обязательность контроля:

неотъемлемой частью работ по обеспечению кибербезопасности является оценка эффективности системы защиты. 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.

- Контроль со стороны руководства:

руководство Компании на регулярной основе (не реже одного раза в год) рассматривает отчеты о состоянии кибербезопасности в Компании и фактах нарушений установленных требований, а также общие и частные вопросы кибербезопасности, связанные с использованием технологий повышенного риска или существенно влияющие на бизнес-процессы. Политика кибербезопасности и предложения по ее актуализации рассматриваются Руководством.

- Целевое финансирование мероприятий по обеспечению кибербезопасности:

ежегодный бюджет Компании предусматривает специальные статьи расходов на обеспечение кибербезопасности.

5.2. Принципы контроля состояния систем обеспечения кибербезопасности

- Для обеспечения высокого уровня контроля в отношении системы управления кибербезопасностью в Компании проводится комплексный анализ существующих защитных механизмов и возникающих инцидентов кибербезопасности, а также ежегодный полный аудит всей системы защиты информации;
- Процесс мониторинга состояния кибербезопасности включает в себя контроль качества функционирования организационных и технических защитных мер, анализ параметров конфигурации и настройки защитных механизмов;
- С целью оперативного выявления инцидентов кибербезопасности и действий в информационных системах, которые могут привести к реализации угроз кибербезопасности, в Компании определены процедуры мониторинга и анализа данных о зарегистрированных событиях кибербезопасности;
- Внутренние и внешние аудиты или самооценки выполняются по возможности силами доверенных подготовленных независимых аудиторов или сотрудниками ЦКЗ;
- По результатам аудита уполномоченные работники ЦКЗ и ответственные подразделения Компании в разумные сроки определяют действия, необходимые для устранения обнаруженных несоответствий в процессе аудита и вызвавших их причин.

6. ВНЕСЕНИЕ ИЗМЕНЕНИЙ

6.1. Внесение изменений в Политику организует директор ЦКЗ при наступлении одного из следующих условий:

- при необходимости по результатам анализа рисков, аудитов и проверок соответствия требованиям кибербезопасности;
- получения сообщения о необходимости внесения изменений в документ от любого участника процесса, обнаружившего несоответствие в нем;
- распоряжения Руководства Компании;
- проведения организационных и структурных изменений в Компании, затрагивающих процессы управления кибербезопасности;
- в связи с внесением изменений в законодательство;
- в связи с внесением изменений во внутренние документы Компании.

6.2. В целях поддержания актуальности и эффективности действий по обеспечению кибербезопасности данный документ должен пересматриваться не реже одного раза в год.

6.3. Ответственный за соблюдение периода пересмотра документа является директор ЦКЗ.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

N версии документа	Содержание изменения	Ф.И.О. ответственного лица, внёсшего	Дата внесения изменения
1.1	Добавление информации о соответствии требованиям международного стандарта ISO/IEC 27701:2019.	Коршикова Ю.И.	24.09.2021