ТОО «Интернет-компания PS»

Политика информационной безопасности

Версия от 11.04.2022

www.ps.kz

1. Общие положения

Настоящая Политика информационной безопасности ТОО «Интернет-компания PS» (далее — Политика) определяет систему принципов обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в ТОО «Интернет-компания PS» (далее — Компания).

Обеспечение информационной безопасности Компании осуществляется в рамках циклической модели менеджмента информационной безопасности: «планирование — реализация — проверка — совершенствование».

Политика является общедоступным документом, который может предоставляться без ограничений всем заинтересованным лицам.

Информационная безопасность (далее — ИБ) — состояние информационной системы, при котором невозможен несанкционированный доступ, использование, раскрытие, искажение, изменение, исследование, запись или уничтожение информации. ИБ подразумевает под собой механизм, регулирующий обмен информацией и соответствующий таким принципам, как: конфиденциальность, доступность и целостность.

Информационная система (ИС) — совокупность технического, программного и технологического обеспечения, а также персонала, обеспечивающая хранение, обработку и выдачу информации в интересах достижения поставленной цели.

Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий в Компании, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит перечень угроз безопасности для объектов и субъектов информационных отношений Компании.

Требования настоящей Политики распространяются на все структурные подразделения Компании.

Политика разработана в соответствии с законами и нормативными правовыми актами Республики Казахстан (далее — РК).

Политика является методологической основой для:

1. формирования и соблюдения единых политик в области обеспечения безопасности информации в Компании;
2. организации работ по выявлению информации, подлежащей защите, обоснованию уровня ее конфиденциальности и документальному оформлению в виде соответствующих перечней;
3. принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации;
4. выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
5. координации деятельности структурных подразделений Компании при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;
6. разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в Компании.

Защита информационных ресурсов осуществляется в рамках системы управления ИБ, соответствующей:

- требованиям стандартов ISO/IEC 27001:2013 и СТ РК ISO/IEC 27001-2015: «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;
- требованиям законодательства РК, нормативным и договорным обязательствам Компании с точки зрения информационной безопасности;
- настоящей Политике информационной безопасности Компании.

Областью действия системы управления информационной безопасностью (далее — СУИБ) Компании является успешное предоставление, сопровождение и поддержание услуг обработки данных и услуг по обеспечению инфраструктурой для размещения данных и информационных технологий.

Руководство Компании, в лице генерального и исполнительного директоров, полностью берет на себя ответственность за деятельность по обеспечению ИБ в Компании, декларирует свою приверженность вышеуказанным целям и принципам, а также обязывает к этому весь персонал Компании. Сотрудники Компании несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области ИБ.

Политика направлена на достижение основных целей:

1. защиту целостности информации, используемой и обрабатываемой в рамках области сертификации;

2. сохранение конфиденциальности критичных информационных ресурсов;
3. обеспечение доступности обрабатываемой информации в ИС Компании;
4. обеспечение непрерывности основных бизнес-процессов, функционирующих в рамках области сертификации;
5. сокращение времени реагирования на инциденты ИБ;
6. повышение качества оказываемых услуг.

Для достижения указанных целей необходимо решение следующих задач:

1. активного участия руководства в управлении ИБ Компании;
2. повышения осведомленности сотрудников и, где применимо, подрядчиков в области рисков, связанных с информационными ресурсами;
3. четкого распределения ответственности и обязанностей сотрудников по обеспечению ИБ;
4. разграничения доступа сотрудников к аппаратным, программным и информационным ресурсам Компании;
5. регистрации действий пользователей в системных журналах при использовании сетевых ресурсов;
6. контроль корректности действий пользователей систем путем анализа содержимого этих журналов;
7. защиты от вмешательства посторонних лиц в процесс функционирования ИС;
8. контроля целостности используемых программных средств, среды исполнения программ и ее восстановление в случае нарушения, а также защиты систем от внедрения вредоносных кодов;
9. защиту информации с ограниченным распространением, персональных данных от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
10. обеспечения аутентификации пользователей ИС и ресурсов;
11. своевременного выявления угроз ИБ, причин и условий, способствующих нанесению ущерба;
12. создания условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц;
13. введение практики дисциплинарного взыскания в случае нарушения Политики;
14. ликвидации последствий нарушения ИБ;
15. разработки и внедрения правил и инструкции по обеспечению ИБ, контроля исполнения соответствующих требований сотрудниками Компании;
16. реализации мероприятий по оценке, управлению и минимизации информационных рисков;
17. непрерывное совершенствование СУИБ.

2. Ответственность и обязательства руководства

Эффективная безопасность требует подотчетности, исчерпывающего определения и признания обязанностей в сфере безопасности. Руководство должно отвечать за все аспекты управления безопасностью, включая принятие решений по управлению рисками. Отдельные ее факторы, такие как тип, форма регистрации, размер и структура Компании, повлияют на то, на каком уровне будут определены эти обязанности. Надлежащее определение и разграничение подотчетности, специфических служебных обязанностей и ответственности должно обеспечивать эффективное и квалифицированное выполнение всех важных задач.

Руководство принимает непосредственное участие в решении вопросов, связанных с обеспечением ИБ в соответствии с целями деятельности Компании (бизнеса), законами и нормативными актами.

Руководство осуществляет поддержку заданного уровня ИБ путем внедрения СУИБ, а также путем распределения обязанностей и ответственности персонала за ее обеспечение.

Руководство должно:

1. формулировать, пересматривать и утверждать Политику ИБ, а также следить за эффективностью ее реализации;
2. обеспечивать четкое управление и реальную поддержку инициатив в области ИБ;
3. предоставлять ресурсы для обеспечения ИБ;
4. обеспечивать координацию мер контроля ИБ Компании;
5. закреплять обязанности сотрудников по ИБ в Компании посредством должностных инструкций, приказов, указов и т.д.;
6. инициировать идеи, планы и программы по поддержанию осведомленности об ИБ, определять потребность обучения сотрудников и, при необходимости, подрядчиков Компании методам и процедурам обеспечения безопасности, определять обязанности, относящиеся к установке и обслуживанию программного обеспечения и аппаратной части;
7. определять потребность в консультации специалиста внутри Компании или со стороны по вопросам ИБ, и контролировать результаты консультаций по всей Компании;

8. четко устанавливать ответственность руководителей подразделений за различные активы и процессы безопасности, детали этой ответственности должны быть документированы, уровни полномочий должны быть ясно определены и документированы;
9. ввести практику дисциплинарного взыскания в случае нарушения Политики;
10. ликвидировать последствия нарушения ИБ;
11. обязательно и своевременно выявлять, пресекать попытки нарушения установленных правил обеспечения ИБ.

Контроль деятельности пользователей, 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.

Сотрудники должны быть ознакомлены с мерами ответственности за разглашение информации в соответствии с их функциональными обязанностями, а также с мерами ответственности за возможные нарушения.

3. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения ИБ в Компании являются:

1. соблюдение требований законодательства Республики Казахстан;
2. соответствие международным и национальным стандартам в области ИБ, действующим на территории Республики Казахстан;
3. постоянный и всесторонний анализ информационного пространства с целью выявления уязвимостей информационных активов;
4. выявление причинно-следственных связей возможных проблем и построение на этой основе точного прогноза их развития;
5. оценка степени влияния выявленных проблем;
6. комплексное использование методов и средств защиты компьютерных систем, перекрывающих все существенные каналы реализации угроз и не содержащих слабых мест на стыках отдельных ее компонентов, защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами, при этом меры, принимаемые для обеспечения ИБ, не должны усложнять достижение уставных целей, а также повышать трудоемкость технологических процессов обработки информации;
7. эффективная реализация принятых защитных мер;
8. гибкость средств защиты для обеспечения ИБ Компании в случае возможных изменений внешних условий и требований с течением времени;
9. совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования ИС с учетом изменений в методах и средствах перехвата информации и воздействия на их компоненты, нормативных требований по защите и опыта как отечественных, так и зарубежных организаций достигнутого в этой области;
10. непрерывность принципов безопасного функционирования;
11. обязательность и своевременность выявления, пресечение попыток нарушения установленных правил обеспечения ИБ;
12. четкое определение функциональных целей и целей ИБ в документах во избежание неопределенности в организационной структуре, ролях персонала, утвержденных политиках и невозможности оценки адекватности принятых защитных мер;
13. определение персональной ответственности за обеспечение безопасности информации и системы ее обработки для каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников должно быть построено таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму;
14. обеспечение доступности услуг и сервисов для своих клиентов и контрагентов в сроки, установленные соответствующими договорами (соглашениями) и/или иными документами;
15. наблюдаемость и возможность оценки обеспечения ИБ, результат применения защитных мер должен быть явно наблюдаем (прозрачен) и оценен специалистом, имеющим соответствующие полномочия;
16. классификация обрабатываемой информации, определение уровня ее важности в соответствии с законодательством РК.

4. Правила пересмотра

Политика ИБ, а также вся документация по СУИБ Компании, в соответствии с постановлением Правительства РК “Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности”, требует регулярного пересмотра и корректировки не реже одного раза в два года.

Внеплановый пересмотр документации СУИБ проводится в случае:

1. внесения существенных изменений в организационную структуру Компании;
2. изменений в законодательстве РК;
3. возникновения инцидентов ИБ.

При внесении изменений учитываются следующие входные данные:

1. результаты аудита ИБ, а также результаты предыдущих аудитов;
2. рекомендации независимых экспертов по ИБ;
3. существенные угрозы и уязвимости ИС;
4. отчеты об инцидентах в области ИБ;
5. рекомендации органов государственной власти;
6. обратная связь заинтересованных лиц;
7. статус превентивных и корректирующих действий;
8. результаты протоколов руководства по ИБ;
9. процесс производительности и комплаенс с политикой ИБ;
10. изменения, которые могут затронуть подход организации к управлению ИБ, включая изменения организационной сферы, бизнес обстоятельств, доступности ресурсов, контрактные регуляторные требования и техническое окружение;
11. тренды, относящиеся к угрозам и уязвимостям;
12. сообщенные инциденты ИБ.

Пересмотр документации СУИБ осуществляется специалистами, ответственными за ее разработку и внедрение, а также включает в себя оценку возможности улучшения ее положений и процесса управления ИБ в соответствии с изменениями.

Итогом пересмотра руководством документации СУИБ является совершенствование организационного подхода по управлению ИБ, контролей и их целей, распределение ресурсов и обязанностей и т.п.

Документация СУИБ подлежит обязательному пересмотру по результатам проведения анализа и оценки рисков ИБ для ИС и должна актуализироваться по мере необходимости.

Пересмотренная документация СУИБ утверждается руководством Компании.