ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Астана
2023 год

Общее положение

Настоящая Политика информационной безопасности информационной системы реестра Qazaq Green Certificate Registry (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 у оператора Qazaq Green Certificate Registry - Ассоциация ВИЭ «Qazaq Green» (далее – Организация).

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

Требования настоящей Политики распространяются на все структурные подразделения Организации.

Политика разработана в соответствии с Законами Республики Казахстан «Об электронном документе и электронной цифровой подписи», нормативными правовыми актами Республики Казахстан, а также другими нормативными правовыми актами Республики Казахстан.

Политика является методологической основой для:

1) формирования и проведения единой политики в области обеспечения безопасности информации в Организации;

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 Организации 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 Организации.

Защита информационных ресурсов осуществляется в рамках Системы управления информационной безопасностью, соответствующей:

- требованиям стандарта по информационной безопасности СТ РК ИСО/МЭК 27001-2015.
- требованиям законодательства Республики Казахстан, нормативным и договорным обязательствам Организации с точки зрения информационной безопасности;
- настоящей Политике информационной безопасности Организации.

Областью действия Системы управления информационной безопасностью Организации является: управления информационной безопасностью в отношении бесперебойного функционирования информационных систем Организации.

Руководство Организации полностью берет на себя ответственность за деятельность по обеспечению информационной безопасности в Организации, декларирует свою приверженность вышеуказанным целям и принципам, а также обязывает к этому весь персонал Организации. Работники Организации несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности

Данная Политика построения Системы управления информационной безопасностью подлежит регулярному, не реже одного раза в год, пересмотру.

Политика направлена на достижение основных целей:

1) защиту целостности информации, используемой и обрабатываемой в Организации;
2) сохранение конфиденциальности критичных информационных ресурсов;
3) обеспечение доступности обрабатываемой информации для зарегистрированных пользователей;
4) обеспечение непрерывности основных бизнес-процессов, функционирующих в Организации.

Для достижения указанных целей необходимо решение следующих задач:

1) активного участия руководства в управлении информационной безопасностью предприятия;
2) повышения осведомленности сотрудников в области рисков, связанных с информационными ресурсами;
3) четкого распределения ответственности и обязанностей сотрудников по обеспечению информационной безопасности;

4) разграничения доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам предприятия;

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 информационных систем;

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 информационных систем и ресурсов;

11) своевременного выявления угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

12) создания условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц;

13) ведение практики дисциплинарного взыскания в случае нарушения Политики информационной безопасности;

14) ликвидации последствий нарушения информационной безопасности;

15) разработки и внедрения правил и инструкции по обеспечению информационной безопасности, контроля исполнения соответствующих требований сотрудниками предприятия;

16) реализации мероприятий по оценке и управлению информационными рисками;

17) совершенствование системы управления информационной безопасностью.

1. 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 организации, повлияют на то, на каком уровне будут определены эти обязанности. Информационная безопасность –

это междисциплинарная тема, относящаяся ко всем пользователям внутри Предприятия. 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 информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами.

Руководство осуществляет поддержку заданного уровня информационной безопасности путем внедрения системы менеджмента, а также путем распределения обязанностей и ответственности персонала за ее обеспечение (приказ о назначении ответственных лиц, должностные инструкции и т.д.).

Руководство:

1. формулировать, пересматривать и утверждать политику информационной безопасности, а также следить за эффективностью реализации политики информационной безопасности;
2. обеспечивать четкое управление и реальную поддержку инициатив в области информационной безопасности;
3. предоставлять ресурсы для обеспечения информационной безопасности;
4. обеспечивать координацию мер контроля информационной безопасностью в организации;
5. утверждать роли и обязанности сотрудников по информационной безопасности в организации посредствам должностных инструкций, приказов, указов и т.д.;
6. инициировать идеи, планы и программы по поддержанию осведомлённости об информационной безопасности, определять потребность обучения пользователей и администраторов методам и процедурам обеспечения безопасности, определять обязанности, относящиеся к установке и обслуживанию программного обеспечения и аппаратной части;
7. определять потребность в консультации специалиста внутри организации или со стороны по вопросам информационной безопасности, просматривать и координировать результаты консультации по всей организации;

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 (акт о материальной ответственности);

9. ведение практики дисциплинарного взыскания в случае нарушения Политики информационной безопасности;

10. ликвидации последствий нарушения информационной безопасности.

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

Обслуживающий персонал ИС при нарушении требований пунктов политики ИБ будет привлекаться к административной или иной ответственности, в соответствии с действующим законодательством Республики Казахстан. Ответственность на администраторов ИС возлагается в соответствии с их ответственностью согласно Инструкции по закреплению функций и полномочий администратора сервера. В частности, администраторы ресурсов ИС обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

3. Основные принципы обеспечения информационной безопасности

Основными принципами обеспечения информационной безопасности являются:

1) соблюдение требований законодательства Республики Казахстан;

2) соответствие международным и национальным стандартам в области информационной безопасности, 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) адекватная 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 информационной безопасности, 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 варьирования уровнем защищенности в связи с возможными изменениями внешних условий и требований с течением времени;

9) совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, анализа функционирования информационных систем с учетом изменений в методах и средствах перехвата информации и воздействия на их компоненты, нормативных требований по защите, достигнутого этой области опыта других организаций, как отечественных, так и зарубежных;

10) непрерывность принципов безопасного функционирования.

11) обязательность и своевременность выявления, пресечение попыток нарушения установленных правил обеспечения информационной безопасности. Контроль деятельности пользователей, каждого средства зашиты 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;

12) четкое определение функциональных целей и целей информационной безопасности в документах во избежание неопределенности в организационной структуре, ролей персонала, утвержденных политик 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 для своих клиентов и контрагентов услуг и сервисов в установленные сроки, определенные соответствующими договорами (соглашениями) и/или иными документами;

15) наблюдаемость и возможность оценки обеспечения информационной безопасности, результат применения защитных мер должен быть явно наблюдаем (прозрачен) и мог быть оценен специалистом, имеющим соответствующие полномочия;

16) классификация обрабатываемой информации, определение уровня ее важности в соответствии с законодательством Республики Казахстан.

4. Кадровая политика по обеспечению информационной безопасности

Функции и обязанности персонала четко определены в должностных инструкциях и сообщены кандидатам при приеме на работу.

Сотрудники подписывают условия трудового договора, в котором установлены их ответственность и ответственность предприятия относительно информационной безопасности.

Сотрудники и представители сторонних организаций, использующие средства обработки информации организации, должны подписать соглашение в соответствии с требованиями информационной безопасности в целях снижения рисков от воровства, мошенничества и нецелевого использования оборудования, а также от угроз безопасности информации.

Соглашение о соблюдении конфиденциальности и неразглашении подписывается сотрудником, подрядчиком или пользователем сторонней организацией до предоставления доступа к средствам обработки информации.

Проверка всех кандидатов на постоянную работу должна быть проведена в соответствии с действующим трудовым законодательством РК с соблюдением конфиденциальности личных данных. Проверке подлежит следующая предоставляемая кандидатом информация:

1) рекомендации с предыдущих мест работы;
2) резюме претендента;
3) документы об образовании и профессиональных квалификациях;
4) документы, удостоверяющие личность;
5) прочая информация, требующая уточнений.

Информация обо всех сотрудниках, принимаемых в постоянный штат, должна быть собрана и обработана в соответствии с действующим трудовым законодательством РК.

Сотрудники должны быть ознакомлены с требованиями настоящей Политики, правилами и инструкциями по обеспечению информационной безопасности, с обязательным подписанием листа ознакомления, в целях повышения осведомленности, информирования о процедурах реагирования на инциденты и их предотвращения.

Необходимо осуществлять контроль возврата всех активов (средства вычислительной техники, служебные документы, электронные носители и т.д.), находящихся в пользовании сотрудников по окончании действия их трудового договора, а также, в случае использования сотрудником личного

оборудования, обеспечить передачу информации руководителю соответствующего подразделения (ответственному специалисту) или удаление информации с оборудования невосстанавливаемыми методами.

Права доступа к информационным системам и ресурсам аннулируются по окончании действия трудового договора (увольнения) сотрудника или подлежат пересмотру при изменении его обязанностей и функций.

Пароли для учетных записей, оставшихся активными, должны быть изменены на момент прекращения трудовой деятельности, вызванной в связи с длительной командировкой, отпуском или окончания действия трудового договора.

5. Пересмотр Политики информационной безопасности

Положения политики информационной безопасности Предприятия требуют регулярного пересмотра и корректировки не реже одного раза в год согласно плану.

Внеплановый пересмотр Политики безопасности проводится в случае:

1) внесения существенных изменений в ИС;
2) измененияими в законодательстве, организационной структуре;
3) возникновения инцидентов информационной безопасности.

При внесении изменений учитываются:

1) результаты аудита информационной безопасности, а также результаты предыдущих аудитов;
2) рекомендации независимых экспертов по информационной безопасности;
3) существенные угрозы и уязвимости информационной системы;
4) отчеты об инцидентах в области информационной безопасности;
5) рекомендации органов государственной власти.

Пересмотр Политики осуществляется специалистами, ответственным за ее разработку, внедрение и включает оценку возможности улучшения ее положений и процесса управления информационной безопасностью в соответствии с изменениями.

Пересмотр политики информационной безопасности должен осуществляться в соответствии с руководством по реализации СТ РК ИСО/МЭК 27002-2009.

Настоящая Политика подлежит обязательному пересмотру по результатам проведения анализа и оценки рисков информационной безопасности для ИС и должна актуализироваться по мере необходимости.

Пересмотренная политика информационной безопасности утверждается уполномоченными лицами.

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Личная подпись	Дата
1	**2**	**3**	**4**	**5**
1				
2				
3				
4				
5				
6				
7				
8				
9				