Утверждаю
Председатель Правления
АО «Шардаринская ГЭС»
_____А. Берлибаев
«_04_» _____09_____ 2023 г.

Политика информационной безопасности АО «Шардаринская ГЭС»

Шардара

1. Введение

1. Настоящая Политика информационной безопасности АО «Шардаринская ГЭС» (далее - Политика) - это документ в области защиты информации АО «Шардаринская ГЭС» (далее – Общество), определяющий цели, задачи, основные принципы, общие направления и требования обеспечения информационной безопасности в деятельности Общества и на всех участках его информационных и телекоммуникационных систем с учетом особенностей деятельности Общества, его организационной структуры и размещения информационных систем и характера решаемых Обществом задач.

2. Обеспечение информационной безопасности Общества является необходимым условием для успешного выполнения уставных целей и задач Общества и нарушения в данной области могут привести к серьезным последствиям, включая потерю активов, деловую репутацию перед партнерами и снижение конкурентоспособности Общества.

3. Политика обеспечивает процессы информационной безопасности и ответственность за их выполнение. На основе Политики строится вся организационно-распорядительная документация и все процессы обеспечения информационной безопасности Общества.

4. Политика разработана на основании следующих нормативных правовых актов Республики Казахстан:

1) Закон Республики Казахстан «Об информатизации»;

2) Закон Республики Казахстан «Об электронном документе и электронно-цифровой подписи»;

3) Концепция кибербезопасности «Киберщит Казахстан»;

4) СТ РК ISO/IEC 27001-2015 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасностью. Требования»;

5) СТ РК ИСО/МЭК 17799-2006 «Информационные технологии. Методы обеспечения защиты. Свод правил по управлению защиты информации».

2. Термины и определения

5. В настоящей Политике применяются в соответствии с законами Республики Казахстан «Об информатизации», «Об электронном документе и электронно-цифровой подписи» и внутренними нормативными документами Общества следующие определения и сокращения:

1) **Общество** - АО «Шардаринская ГЭС»;

2) **руководящие работники Общества** - Председатель Правления и заместители Председателя Правления;

3) **Совет директоров** - орган управления Общества;

4) **системный администратор** - уполномоченный работник Общества, обеспечивающий функционирование соответствующих механизмов, а также работник подрядной организации, оказывающий услуги согласно

заключенному договору по администрированию общей информационной системы Общества;

5) **пользователь** - работник Общества, а также третье лицо, имеющее доступ к информационным ресурсам Общества, обращающиеся к информационным системам за получением необходимых электронных информационных ресурсов и пользующиеся ими;

6) **информационная безопасность (ИБ)** - комплекс правовых, организационно-распорядительных и технических мер, направленных на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе ее сбора, обработки, передачи, хранения и пользования;

7) **СУИБ** - система управления информационной безопасностью.

3. Цели и задачи Политики

6. Основной целью Политики является защита информационных ресурсов и информационных систем Общества от возможного нанесения им ощутимого материального, физического, морального или иного ущерба посредством случайного или злонамеренного несанкционированного вмешательства в процесс функционирования информационных систем Общества или несанкционированного доступа к циркулирующей в них информации и ее незаконного использования.

7. Основными задачами Политики являются:

1) обеспечение необходимой доступности информационных ресурсов Общества в целях обеспечения непрерывности бизнеса;

2) обеспечение целостности информационных ресурсов Общества в целях обеспечения требуемой поддержки деятельности Общества в информационной сфере, включая задачи принятия решений;

3) обеспечение конфиденциальности информации, отнесенной к закрытым сведениям Общества;

4) обеспечение достоверности и актуальности обрабатываемой информации;

5) установление ответственности за использование информационных активов Общества и управления ими;

6) применение обоснованных, экономически выгодных и совместимых организационных и технических мер информационной безопасности, как для информационных технологий, так и для Общества в целом;

7) утверждение единой корпоративной этики в вопросах информационной безопасности, поддерживающей осведомленность работников;

8) защита прав и законных интересов Общества и работников, в случаях неправомерного использования или злоупотребления информационными активами;

9) защита от несанкционированных действий в процессах функционирования информационных систем;

10) разграничение прав доступа к информации, серверам и рабочим станциям, средствам защиты.

4. Принципы Политики

8. Политика предполагает следующие принципы построения комплексной системы защиты информационной безопасности Общества:

1) **законность** - осуществление защитных мероприятий и разработку системы безопасности информации Общества в соответствии с действующим законодательством Республики Казахстан;

2) **системность** - определённая последовательность и упорядоченность защиты информации и учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения безопасности информации;

3) **комплексность** - согласованное применение разнородных методов и средств защиты компьютерных систем при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов;

4) **непрерывность защиты** - непрерывный процесс соответствующих мер на всех этапах жизненного цикла информационных систем;

5) **своевременность** - принятие упреждающих мер для обеспечения безопасности информации;

6) **преемственность и совершенствование** - построение единой содержательной линии, обеспечивающей эффективное поступательное развитие мер и средств защиты информации;

7) **конфиденциальность** - защита от несанкционированного ознакомления с информацией;

8) **достоверность** - общая точность и полнота информации;

9) **разграничение ответственности и контроля** - определение прав и обязанностей работников и иных пользователей за выполнение тех или иных задач и осуществление контроля в сфере информационной безопасности.

5. Угрозы безопасности информационных и телекоммуникационных средств и систем

9. Основными угрозами безопасности информационных и телекоммуникационных средств и систем в Обществе могут являться:

1) несанкционированный доступ к информации, обрабатываемой, хранимой и передаваемой в информационных и телекоммуникационных системах Общества;

2) нарушения технологии обработки информации;

3) внедрение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;

4) уничтожение, повреждение или разрушение средств и систем обработки информации, телекоммуникации и связи;

5) воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;

6) уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

7) перехват информации в сетях передачи данных и на линиях связи, обработка этой информации и навязывание ложной информации.

10. Основными источниками угроз информационной безопасности являются:

1) деятельность организаций, групп и отдельных лиц, направленная на получение несанкционированного доступа к информации и осуществление контроля за функционированием информационных и телекоммуникационных систем Общества;

2) вредоносное программное обеспечение;

3) преднамеренные действия и ошибки работников информационных и телекоммуникационных систем, отказ технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах.

6. Меры защиты информационных ресурсов и информационных систем

11. Безопасное функционирование Общества должно основываться на своевременности обнаружения проблем в сфере информационной безопасности, потенциально способных повлиять на бизнес-цели Общества, выявлении причинно-следственных связей возможных проблем и создании на этой основе точного прогноза их развития.

12. Общество выбирает эффективные защитные меры, адекватные реальным угрозам, с учетом затрат на реализацию таких мер и объема возможных потерь от реализации угроз. При этом необходимо учитывать, что должны применяться только такие защитные меры, правильность работы которых может быть проверена. Также необходима регулярная оценка адекватности защитных мер и эффективности их реализации с учетом влияния защитных мер на бизнес-цели Общества.

13. Для защиты информационных ресурсов и систем Обществом осуществляются следующие меры:

1) **правовые меры защиты** – меры, заключаемые собственником/владельцем информационных ресурсов с пользователями информации договоры, в которых устанавливаются условия доступа к определенным информационным ресурсам и ответственность за нарушение условий доступа и использования информационных ресурсов;

2) **организационные меры защиты** - обеспечение особого режима допуска на территории (в помещения), где может быть осуществлен доступ к

информации (к материальным носителям информации), а также разграничение доступа к информации по кругу лиц и характеру информации;

3) **морально-этические меры** - в Уставе, Кодексе корпоративного управления и Кодексе поведения Общества, на основании Закона Республики Казахстан «Об акционерных обществах», определены обязательные нормы поведения для работников Общества, нарушения которых могут повлечь не только падение авторитета отдельного работника, но и репутации и информационной безопасности всего Общества в целом;

4) **технические меры защиты** - физической защите информационных систем, использование средств защиты информации, в том числе систем контроля доступа и регистрации фактов доступа к информации.

14. Обществом принимаются следующие меры по защите информационных каналов:

1) обеспечение целостности и сохранности информационных ресурсов, недопущение их несанкционированного изменения или уничтожения;

2) соблюдение конфиденциальности информационных ресурсов ограниченного доступа;

3) реализация права на доступ к информационным ресурсам;

4) недопущение несанкционированного воздействия на средства обработки и передачи информационных ресурсов.

15. Обществом принимаются следующие меры по защите информационных ресурсов и систем, направленных на недопущение несанкционированных действий, приводящих к:

1) блокированию информационных ресурсов, то есть совершению действий, приводящих к ограничению или закрытию доступа к информационной системе и предоставляемым ею информационным ресурсам;

2) модификации информационных ресурсов, то есть внесению изменений в программы, базы данных, текстовую информацию, находящуюся на материальном носителе;

3) копированию информационного ресурса, то есть переносу информации на другой материальный носитель;

4) использованию программных продуктов без разрешения правообладателя;

5) нарушению работы информационных систем и (или) программных продуктов либо нарушению функционирования корпоративной сети.

16. Обществом принимаются следующие меры по физической защите информационно-технических ресурсов:

1) элементы информационной системы, потенциально подверженные ущербу, размещаются в защищенных зонах; уровень защищенности зоны должен соответствовать потенциальным угрозам в отношении информационно-технических ресурсов внутри неё;

2) осуществление контроля доступа в защищенные зоны и к критическим элементам информационных и телекоммуникационных систем; степень контроля должна соответствовать значимости защищаемых компонентов;

3) осуществление контроля основных параметров вспомогательных систем, обеспечивающих функционирование информационных и телекоммуникационных систем (надежность и качество электроснабжения, климатические условия и т.д.).

7. Данные, документация и программное обеспечение

17. Вся информация, хранимая, разработанная, обрабатываемая и передаваемая по каналам связи в информационных и телекоммуникационных системах Общества, которая не была специально идентифицирована как собственность третьих сторон, является собственностью Общества. Запрещается несанкционированный доступ к информации, разработанной, обрабатываемой, хранимой и передаваемой в информационных системах Общества, ее раскрытие, передача, копирование, изменение, удаление, ненадлежащее использование, а также неправомерное обращение с носителями этой информации. Кроме того, Общество защищает принадлежащую третьим сторонам информацию, переданную Обществу на условиях конфиденциальности.

18. Программное обеспечение, документацию, а также внутреннюю информацию Общества запрещается передавать любыми способами внешним по отношению к Обществу сторонам с целями, отличными от целей решения производственных задач, выполнение которых осуществляется с соответствующего разрешения руководящих работников Общества.

19. Установка, удаление и конфигурирование программного обеспечения на рабочих станциях пользователей корпоративной сети Общества осуществляется только Системным администратором. Пользователям запрещается самостоятельно выполнять указанные действия.

20. Общество строго соблюдает лицензионные соглашения с поставщиками программного обеспечения и владельцами прав на интеллектуальную собственность. Общество разрешает воспроизводить материалы, защищенные правом на интеллектуальную собственность, только в той степени, которая юридически рассматривается как «законное использование» или с разрешения автора/владельца.

21. Любые информационные ресурсы, которые хранятся или обрабатываются на компьютерах, принадлежащих Обществу, являются собственностью Общества, которое оставляет за собой право на изучение всех данных, хранимых, обрабатываемых и передаваемых по каналам связи в Обществе и их изъятие уполномоченными на то лицами Общества.

8. Пользователь, должностные обязанности работников, обучение информационной безопасности

22. Решение вопросов обеспечения безопасности, направлено на уменьшение риска реализации событий, обусловленных ошибками

работников, кражами информационных и технических ресурсов, мошенничеством или незаконным использованием ресурсов работниками Общества и иными пользователями.

23. Пользователь должен быть обучен процедурам защиты и правильному обращению с информационными ресурсами Общества.

24. Пользователь должен получить необходимые сведения о правилах и определенных в Обществе процедурах, включая требования к безопасности и другим средствам контроля, а также научиться правильно использовать информационные ресурсы и сервисы информационных систем.

25. Политикой должны руководствоваться как работники Общества, так и пользователи информационных систем из сторонних организаций, имеющих постоянный или временный доступ к информационным ресурсам Общества.

9. Защита удаленного доступа и мобильного оборудования

26. Обеспечение работникам Общества, его партнерам и клиентам защищенного удаленного авторизованного доступа к соответствующим (и разрешенным) корпоративным информационным ресурсам должно быть санкционировано руководящими работниками Общества. На удаленных и переносных компьютерах должны использоваться персональные межсетевые экраны и VPN-технологии на основе стандартов IPSec или SSL.

27. Системный администратор должен осуществлять проверку на соответствие необходимым требованиям безопасности программного обеспечения удаленных рабочих станций и переносных компьютеров до предоставления им доступа в сеть. Для удаленных рабочих станций это осуществляется за счет установки на них соответствующих клиентских программ, которые позволяют обеспечить проверку программного обеспечения, используемого на удаленной станции, подключаемой к корпоративной сети, что дает возможность контролировать другие заданные параметры станций. Работникам, использующим персональные компьютеры вне пределов Общества, запрещается их использование для доступа к корпоративным сетевым ресурсам, если на них не установлены средства организации VPN и персональный межсетевой экран, а также антивирусные средства проверки файлов и сообщений электронной почты с последними обновлениями.

28. Во время поездок запрещается оставлять оборудование и носители информации в общедоступных местах без присмотра. Портативные компьютеры и носители информации следует провозить в качестве ручного багажа.

29. Во время поездок портативные компьютеры уязвимы по отношению к кражам, потере и несанкционированному доступу. Для таких компьютеров следует обеспечить надлежащую защиту доступа, чтобы предотвратить несанкционированный доступ к хранящейся в них информации.

10. Система управления информационной безопасностью в Обществе

30. Система управления информационной безопасностью в Обществе является неотъемлемой частью общей системы управления Общества.

31. СУИБ включает в себя систему распределения ролей и ответственности, систему документации, процессы и меры в области обеспечения информационной безопасности и определенную этими процессами и мерами деятельность работников – участников процессов СУИБ и информационные активы.

32. Целью СУИБ является полная и эффективная реализация Обществом настоящей Политики и документов в ее поддержку путем определения, планирования, внедрения, функционирования, мониторинга, оценки результатов и эффективности, поддержки и совершенствования процессов, организационных и технических мер по обеспечению ИБ.

33. В задачи СУИБ входят:

1) выработка критериев оценки активов и рисков, и обеспечение приемлемого уровня рисков Общества в информационных технологиях;

2) внедрение единого подхода к управлению рисками Общества с учетом рекомендаций международных стандартов и лучших практик;

3) внедрение и совершенствование процессного подхода к управлению ИБ в Обществе;

4) эффективное управление процессами обеспечения ИБ;

5) создание и поддержка системы документации по обеспечению ИБ;

6) обеспечение прозрачности процесса управления ИБ для руководящих работников Общества;

7) выработка формальных критериев, необходимых для оценки результативности и эффективности процессов и мер по обеспечению ИБ и принятия решений по их совершенствованию и развитию руководящими работниками Общества.

34. СУИБ строится как измеримый (то есть позволяющий оценивать результаты и эффективность процессов и мер на всех этапах на основе формализованных критериев), непрерывный и циклический процесс, последовательно проходящий следующие стадии:

1) планирования;

2) внедрения;

3) проверки;

4) выполнения.

35. Схематично модель СУИБ Общества приведена на Рисунке 1 (приложение 1 к настоящей Политике).

36. При этом все процессы в рамках СУИБ такие, например, как управление рисками, управление инцидентами и иные, также выстраиваются в рамках этой модели, то есть также проходят циклически четыре стадии.

37. Руководящие работники Общества стремятся поддерживать ежегодный цикл СУИБ в Обществе, при этом цикл отдельных процессов может быть короче и определяется в соответствующих внутренних документах Общества.

38. Ответственность за выполнение отдельных задач, в рамках СУИБ Общества, определена как в настоящей Политике, так и в соответствующих положениях о подразделениях Общества и в должностных инструкциях работников Общества.

39. **Планирование.** Четкое и ясное планирование системы управления, ее процессов, организационных и технических мер по обеспечению ИБ является основой успешной реализации настоящей Политики, которая отражает цели и задачи, намерения руководящих работников Общества, основные принципы в области ИБ, и является предпосылкой планирования.

40. Планирование основывается на оценке рисков Общества в ИБ, а также на оценке результатов и эффективности процессов системы управления и существующих мер по обеспечению ИБ. Планирование системы управления, ее процессов и мер заключается в:

1) определении (пересмотре) подхода к управлению ИБ в Обществе, находящего отражение в настоящей Политике, включая:

а) пересмотр ролей и ответственности, в рамках СУИБ;

б) пересмотр подхода к управлению и оценке рисков Общества в информационных технологиях;

2) оценке достигнутых результатов и эффективности процессов системы управления и существующих мер по обеспечению ИБ, с учетом коррекций, направленных на улучшение и развитие процессов и мер;

3) идентификации и оценке информационных активов, негативное воздействие на которые может повлиять на уровень рисков Общества в сфере ИБ;

4) идентификации и оценке рисков, с учетом результатов процесса управления рисками в ходе предыдущего цикла, оценки результатов процессов и мер;

5) определении (пересмотре) процессов системы управления и мер, планировании и документировании иных процессов и мер, направленных на реагирование на риски, а также на совершенствование и развитие самой СУИБ;

6) прогнозировании уровней остаточного риска в результате внедрения планируемых процессов и мер и их согласование с владельцами бизнес-процессов;

7) определении необходимого объема активов (финансовых, людских и иных) для реализации запланированных процессов и мер по обеспечению ИБ Общества.

41. В соответствии с принципом определенности целей для каждого планируемого процесса или меры, вне зависимости от ее характера, должны быть определены и документированы цели, согласованные с руководящими работниками Общества.

42. Результаты классификации информационных активов и оценки рисков, а также планируемые процессы и меры по реагированию на риски и совершенствованию процессов СУИБ утверждаются руководящими работниками Общества.

43. **Внедрение.** Точное и согласованное внедрение всех запланированных процессов и мер, объективная и обоснованная оценка достижения планируемых результатов и эффективности, повышение осведомленности и обучение всех затрагиваемых планируемыми процессами и мерами лиц является основой достижения, поставленных на этапе планирования, целей.

44. В основе успешного процесса внедрения лежит разработка, согласование и реализация планов по реагированию на риски и совершенствованию СУИБ в Обществе.

45. Принципиальными моментами процесса внедрения являются:

1) соответствие внедряемых процессов и мер результатам этапа планирования;

2) согласование планов со всеми заинтересованными лицами;

3) обеспечение контроля со стороны руководящих работников Общества за сроками и полнотой реализации планов и распоряжением выделенными ресурсами;

4) соответствие планов согласованным бюджетам, а в случае несоответствия – необходимость обоснованной оценки внесения изменений в бюджет и согласование с руководящими работниками Общества;

5) определение четкой и ясной ответственности за реализацию планов или отдельных мероприятий планов.

46. В соответствии с принципом контролируемости для планируемых к внедрению процессов и мер, должны быть разработаны и согласованы с руководящими работниками Общества критерии оценки их результативности и эффективности, при этом результативность процессов и мер оценивается исходя из полноты и качества выполнения запланированных процессов и мер, а эффективность – исходя из степени достижения поставленных целей.

47. Руководящими работниками Общества оцениваются результаты и эффективность внедряемых процессов и мер.

48. Все пересматриваемые и вновь вводимые процессы и меры должны быть документированы и должны отражать цели и задачи процессов и мер, требования к их выполнению, ответственность за выполнение и критерии оценки результативности и эффективности.

49. Необходимо обеспечить разработку программ обучения и повышения осведомленности работников Общества о процессах и мерах, в том числе пересматриваемых и вновь внедряемых, в области ИБ. Программы должны учитывать роль, выполняемую работниками Общества, в рамках системы управления ИБ. В рамках реализации данных программ требуется:

1) определить необходимые требования к квалификации работников Общества, в соответствии с их ролью в СУИБ;

2) оценить эффективность принятых мер по обучению и повышению осведомленности работников Общества;

3) хранить информацию об образовании, прохождении дополнительного обучения, навыках, опыте и квалификации работников Общества;

4) обеспечить уверенность в том, что все работники Общества осведомлены о важности и значимости действий по обеспечению ИБ, знают свои обязанности и ответственность.

50. При реализации планируемых процессов и мер необходимо обеспечить своевременное выявление событий, способных негативно повлиять на результат и эффективность процессов и мер по обеспечению ИБ Общества. Обеспечить своевременное реагирование на эти события, а также на возникающие инциденты ИБ.

51. **Проверка**. Постоянный мониторинг и проверка корректности внедренных процессов и мер, оценка достигнутых результатов и эффективности являются основой уверенности, что все запланированные процессы и меры выполняются в соответствии с требованиями и ожиданиями.

52. Процессы мониторинга и проверки позволяют своевременно обнаруживать различные проблемы, нарушения требований ИБ и инциденты.

53. Руководящие работники Общества должны иметь возможность установить факт соответствия реального и запланированного выполнения процессов и мер.

54. Проверка процессов СУИБ и применяемых организационных и технических мер включает в себя:

1) осуществление непрерывного мониторинга процессов и мер по ИБ, с целью выявления отклонений от их нормального выполнения и недостатков, событий и инцидентов ИБ, которые могут повлиять на риски Общества в ИБ;

2) оценку соответствия выполнения процессов и мер требованиям, предъявляемым к ним на этапе планирования, с целью выявления несоответствий посредством проведения аудитов процессов и мер по ИБ, оценке соответствия со стороны подразделений и лиц, ответственных за реализацию процессов и мер;

3) оценку достигнутых результатов и эффективности, в соответствии с разработанными на этапе внедрения критериями оценки эффективности, поставленными целями и требованиями к процессам и мерам, на основе результатов мониторинга, аудитов и оценки ИБ, управления инцидентами ИБ и мониторинга;

4) переоценку рисков Общества в ИБ с учетом изменений технологий, бизнес-процессов, внешних событий (например, изменений в законодательной среде, изменений социальной обстановки и т.д.), результатов мониторинга, оценки результативности и эффективности, аудитов и оценки соответствия, инцидентов ИБ;

5) регулярное проведение аудита СУИБ и всего комплекса мер по обеспечению ИБ Общества, для обеспечения объективной уверенности руководящими работниками Общества в том, что деятельность по обеспечению ИБ остается адекватной целям и задачам Общества, соответствует как внутренним требованиям, так и требованиям международных стандартов и лучшей практики;

6) накопление информации о лучших практиках в области управления ИБ, методах и средствах обеспечения ИБ с целью их применения в интересах Общества;

7) планирование коррекций и превентивных мер, направленных на устранение несоответствий и последствий инцидентов, а также причин, приведших к их возникновению с учетом накопленных знаний о лучших практиках.

55. При выявлении несоответствий или инцидентов, ключевыми моментами являются:

1) установление причин возникновения этих несоответствий или инцидентов;

2) разработка мер, направленных на устранение причин с целью снижения вероятности повторного возникновения несоответствий или инцидентов;

3) оценка эффективности мер, направленных на устранение как несоответствий и инцидентов, так и причин, приведших к их возникновению.

56. **Выполнение**. Выполнение всех запланированных процессов и мер в соответствии с документированными требованиями к ним является основой успешного достижения поставленных руководящими работниками Общества целей и задач по обеспечению ИБ Общества.

57. Кроме этого, в Обществе должна быть внедрена практика непрерывного совершенствования СУИБ и мер по обеспечению ИБ, с учетом результатов проверки - мониторинга и аудитов, инцидентов, оценки результатов и эффективности внедрения процессов и мер, накопленного опыта и знаний лучших практик на основании разработанных планов коррекций и превентивных мер.

58. В Обществе должны приниматься меры по устранению выявленных проблем и несоответствий требованиям по ИБ в целях недопущения их повторного появления.

11. Информационная безопасность при работе с электронной почтой, в сети Интернет и с документами ограниченного распространения

59. Работникам Общества предоставляются разрешенные правила пользования ресурсами электронной почты (e-mail) Общества. Политика охватывает e-mail, приходящий или отправляемый через все принадлежащие Обществу персональные компьютеры, серверы, ноутбуки, терминалы, карманные переносные компьютеры, сотовые телефоны и любые другие ресурсы, способные посылать или принимать e-mail по протоколам SMTP, POP3, IMAP.

60. Ресурсы сети Интернет используются для получения и распространения информации, связанной с деятельностью Общества, информационно- аналитической работы в интересах Общества, обмена почтовыми сообщениями исключительно с внешними организациями, а также ведения Обществом собственной хозяйственной деятельности.

61. Иное использование ресурсов сети Интернет без разрешения руководства Общества в установленном порядке рассматривается как нарушение информационной безопасности.

62. Процесс управления мониторингом использования ресурсов сети Интернет, как составная часть настоящей Политики, определен в рамках соответствующих регламентирующих процедур, утвержденных локальными актами Общества.

63. Условия соблюдения информационной безопасности при работе с документами ограниченного распространения приведены в соответствующих внутренних документах Общества.

12. Защита от вредоносного программного обеспечения

64. С целью обнаружения и предотвращения проникновения вредоносного программного обеспечения, Обществом проводятся мероприятия по управлению информационной безопасностью, а также формируются процедуры, обеспечивающие соответствующую осведомленность пользователей.

65. Процесс управления защитой от вредоносного программного обеспечения, как составная часть настоящей Политики, определен в рамках соответствующих процедур, утвержденных локальными актами Общества.

13. Оснащение, эксплуатация и доступ к серверному помещению и критическому оборудованию

66. В зданиях Общества используются серверные комнаты. Требования к ним и порядок их эксплуатации прописаны в Регламенте оснащения и эксплуатации серверных помещений.

67. Порядок доступа работников Общества к серверному помещению и критическому оборудованию в Обществе идентичен порядку доступа к сведениям, составляющим конфиденциальную информацию Общества, регламентированному Инструкцией по обеспечению сохранности конфиденциальной информации Общества.

14. Реагирование на инциденты информационной безопасности

68. Пользователи информационных систем Общества должны без промедления сообщать по административным каналам о событиях, потенциально несущих угрозу безопасности, также сообщать все случаи, когда функционирование программного обеспечения представляется им неправильным, т.е. не соответствующим спецификации, подозревая, что сбой вызван вредоносной программой (компьютерным вирусом). Пользователи не должны пытаться самостоятельно восстановить функционирование программного обеспечения путем удаления подозрительного программного обеспечения. Восстановление программного обеспечения должен выполнять Системный администратор.

69. Порядок реагирования пользователей на возникающие в процессе работы инциденты приведен в соответствующих внутренних документах Общества.

15. Заключительные положения

70. Все работники Общества несут ответственность за выполнение требований Политики по обеспечению информационной безопасности доверенных им информационных активов Общества, в соответствии с их должностными и функциональными обязанностями.

71. Внесение изменений и дополнений в настоящую Политику производятся по решению Совета директоров.

Инженер по информационной безопасности — Нурмышев А.Ж.

Согласовано:

Заместитель Председателя Правления – Главный инженер — Сайманов С.М.

Начальник УПБОТОС — Шойбеков Е.И.

Приложение 1
к Политике
информационной
безопасности
АО «Шардаринская
ГЭС»

Рисунок 1. Непрерывный цикл системы управления информационной безопасностью (СУИБ)