N 75/23
от 19.07.2023г.

УТВЕРЖДЕНА
Решением Правления
АО «СПК «Алматы»
Протокол № 37
от «19» 07 2023 года

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «СПК «Алматы»

Владелец	**Служба безопасности**
Разработчик	**Служба безопасности**
Ответственный за хранение экземпляра	**Департамент стратегии и корпоративного развития**
Место хранения подлинника на бумажном и электронном носителе	**База ВНД**
Ответственный за мониторинг и актуализацию	**Служба безопасности Департамент информационных технологий**
Сведения о ВНД, утрачивающих силу в связи с принятием нового	**отсутствуют**
Протокол разногласий	**отсутствуют**
Количество приложений и страниц	**Без приложений, Политика на 20 страницах**

город Алматы
2023 год

СОДЕРЖАНИЕ:

Глава 1. Общие положения

1.1. Настоящий документ - Политика информационной безопасности АО «СПК «Алматы» (далее – Политика) является документом, определяющим приоритеты и принципы обеспечения информационной безопасности в условиях наличия угроз, характерных и существенных для систем и информационных активов АО «СПК «Алматы» (далее – Общество).

1.2. Настоящая Политика разработана в соответствии с законодательством Республики Казахстан в сфере информационной безопасности, серией международных стандартов по информационной безопасности ISO/IEC 27000, COBIT, ITIL, современным состоянием и ближайшими перспективами развития информационной инфраструктуры Общества, а также возможности современных организационно-технических методов защиты информации.

1.3. Политика определяет систему взглядов на обеспечение безопасности информации и представляет собой систематизированное изложение целей и задач защиты, правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, а также основных принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в Обществе.

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

1.5. Политика охватывает все информационные системы и документы, владельцем и пользователем которых является Общества. Обеспечение информационной безопасности – необходимое условие для успешного осуществления деятельности Общества. Информация является одним из важнейших активов Общества.

1.6. Политика является методологической основой для:

- формирования и проведения единой политики в области обеспечения информационной безопасности в Обществе;
- принятия управленческих решений и разработки практических мер по воплощению политики информационной безопасности и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
- координации деятельности структурных подразделений Общества при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению информационной безопасности;
- разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения информационной безопасности в Обществе.

1.7. Использование данной Политики в качестве основы для построения комплексной системы информационной безопасности Общества позволит оптимизировать затраты на ее построение.

1.8. При разработке Политики учитывались основные принципы создания комплексных систем обеспечения безопасности информации, характеристики и возможности организационно-технических методов и современных аппаратно-программных средств защиты и противодействия угрозам безопасности информации.

1.9. Основные положения Политики базируются на качественном осмыслении вопросов информационной безопасности и не затрагивают вопросов экономического (количественного) анализа рисков и обоснования необходимых затрат на защиту информации.

1.10. Положения Политики обязательны для исполнения всеми работниками Общества. Требования Политики также распространяются на другие организации и учреждения, взаимодействие с которыми связано с вопросами информационных ресурсов Общества.

Глава 2. Принципы построения системы информационной безопасности Общества

Построение системы обеспечения безопасности информации Общества и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

2.1. Законность.

Предполагает осуществление защитных мероприятий и разработку системы информационной безопасности Общества в соответствии с действующим законодательством в области информации, информатизации и защиты информации, а также других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.

Все пользователи информационной системы Общества должны иметь представление об ответственности за правонарушения в области информации.

Реализация данного принципа необходима для защиты имени и репутации Общества.

2.2. Системность.

Системный подход к построению системы защиты информации в Обществе предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения информационной безопасности Общества.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места информационной системы Общества, а также характер, возможные объекты и направления атак на нее со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и несанкционированного доступа к информации. Система защиты должна строиться с учетом не только всех известных каналов

проникновения и несанкционированного доступа к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

2.3. Комплексность.

Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами.

2.4. Непрерывность.

Обеспечение информационной безопасности - процесс, осуществляемый Руководством Общества, подразделениями защиты информации и работниками всех уровней. Это процесс, который должен постоянно идти на всех уровнях внутри Общества, и каждый работник Общества должен принимать участие в этом процессе. Деятельность по обеспечению информационной безопасности является составной частью повседневной деятельности Общества. И ее эффективность зависит от участия всех работников Общества в обеспечении информационной безопасности.

Кроме того, большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления защиты.

2.5. Своевременность.

Предполагает упреждающий характер мер обеспечения информационной безопасности, то есть постановку задач по комплексной защите информации и реализацию мер обеспечения безопасности информации на ранних стадиях разработки информационных систем в целом и их систем защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой информационной системы. Это позволит учесть требования безопасности при проектировании и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) системы, обладающие достаточным уровнем защищенности.

2.6. Преемственность и непрерывность совершенствования.

Предполагает постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационной системы Общества и системы ее защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, отечественного и зарубежного опыта в этой области.

2.7. Разумная достаточность (экономическая целесообразность).

Предполагает соответствие уровня затрат на обеспечение безопасности информационных ресурсов и величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения.

2.8. Персональная ответственность.

Предполагает возложение ответственности за обеспечение информационной безопасности и системы ее обработки на каждого работника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей работников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

2.9. Минимизация полномочий.

Означает предоставление пользователям минимальных прав доступа в соответствии со служебной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо работнику для выполнения его должностных обязанностей.

2.10. Исключение конфликта интересов.

Эффективная система обеспечения информационной безопасности предполагает четкое разделение обязанностей работников и исключение ситуаций, когда сфера ответственности работников допускает конфликт интересов. Сферы потенциальных конфликтов должны выявляться, минимизироваться, и находится под строгим независимым контролем. Реализация данного принципа предполагает, что ни один работник не должен иметь полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Наделение работников полномочиями, порождающими конфликт интересов, дает ему возможность подтасовывать информацию в корыстных целях или с тем, чтобы скрыть проблемы или понесенные убытки. Для снижения риска манипулирования информацией и риска хищения, такие полномочия должны в максимально возможной степени быть разделены между различными работниками или подразделениями Общества.

2.11. Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в структурных подразделениях Общества. В такой обстановке работники должны осознанно соблюдать установленные правила и оказывать содействие деятельности подразделений защиты информации.

Важным элементом эффективной системы обеспечения информационной безопасности в Обществе является высокая культура работы с информацией. Руководство Общества несет ответственность за строгое соблюдение этических норм и стандартов профессиональной деятельности, за создание корпоративной культуры, подчеркивающей и демонстрирующей персоналу на всех уровнях важность обеспечения информационной безопасности Общества. Все работники Общества должны понимать свою роль в процессе обеспечения информационной безопасности и принимать участие в этом процессе.

2.12. Гибкость системы защиты.

Система обеспечения информационной безопасности должна быть способна реагировать на изменения внешней среды и условий осуществления Обществом своей деятельности. В число таких изменений входят:

- изменения законодательства, регулирующего отношения в сфере информационной безопасности;
- изменения организационной и штатной структуры Общества;
- корпоративная реструктуризация, расширения, слияния и поглощения;
- изменение существующих или внедрение принципиально новых информационных систем;
- новые технические средства;
- новые виды деятельности, новые услуги, продукты.

Свойство гибкости избавляет в таких ситуациях от необходимости принятия кардинальных мер по полной замене средств и методов защиты на новые, что обеспечивает экономическую эффективность системы обеспечения информационной безопасности.

2.13. Специализация и профессионализм.

Реализация администрирующих мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами Общества (работником Общества, имеющим специальное профильное образование в сфере защиты информации). Допускается привлечение к разработке средств и реализации мер защиты информации специализированных организаций или специалистов, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов и имеющих опыт практической работы.

2.14. Простота первичных приемов защиты для работников.

Механизмы и методы первичных приемов защиты должны быть понятны и просты в использовании. Применение первичных средств и методов защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций.

2.15. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации, на основе используемых систем и средств защиты информации.

Контроль за деятельностью любого пользователя, 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. Кроме того, эффективная система обеспечения информационной безопасности требует наличия адекватной и всеобъемлющей информации о текущем состоянии процессов, связанных с движением информации и сведений о соблюдении установленных нормативных требований, а также дополнительной информации, имеющей отношение к принятию решений. Информация должна быть надежной, своевременной, доступной и правильно оформленной.

Недостатки системы обеспечения информационной безопасности, выявленные работниками Общества или подразделениями обеспечения безопасности должны немедленно доводиться до сведения руководителей соответствующего уровня и оперативно устраняться. О существенных недостатках необходимо сообщать руководству Общества. Руководству ежеквартально направляются отчеты, суммирующие все проблемы, выявленные системой обеспечения информационной безопасности. Подразделением, ответственным за информационную безопасность, ежеквартально не позднее 20 календарных дней после отчетного периода, руководству Общества направляются отчеты, суммирующие все проблемы, выявленные системой обеспечения информационной безопасности.

Глава 3. Субъекты информационных отношении и объекты защиты

3.1. Субъектами информационных отношений при обеспечении информационной безопасности Общества являются:

- Общество, как собственник информационных ресурсов;
- подразделения Общества, участвующие в информационном обмене;
- руководство и работники структурных подразделений Общества, в соответствии с возложенными на них функциями;
- контрагенты Общества - юридические и физические лица, сведения о которых накапливаются, хранятся и обрабатываются в информационной системе Общества;
- другие юридические и физические лица, задействованные в обеспечении выполнения Обществом своих функций (консультанты, разработчики, обслуживающий персонал, организации, привлекаемые для оказания услуг и пр.).

3.2. Перечисленные субъекты информационных отношений заинтересованы в обеспечении:

- своевременного доступа к необходимой им информации (ее доступности);
- достоверности (полноты, точности, адекватности, целостности) информации;
- конфиденциальности (сохранения в тайне) определенной части информации;
- защиты от навязывания им ложной (недостоверной, искаженной) информации;
- разграничения ответственности за нарушения установленных правил обращения с информацией;
- возможности осуществления непрерывного контроля и управления процессами обработки и передачи информации;
- защиты информации от незаконного ее тиражирования (защиты авторских прав, прав собственника информации и т.п.).

3.3. В Обществе циркулирует информация различных уровней конфиденциальности, содержащая сведения ограниченного распространения (служебная, коммерческая, персональные данные), и открытые сведения, которые являются объектами защиты. Защите подлежит вся информация и информационные ресурсы Общества, независимо от ее представления и местонахождения в информационной среде Общества:

1) информационные активы, необходимые для работы Общества, независимо от формы и вида их представления;
2) информационные системы, включая информационные технологии, технические и программные средства формирования, обработки, передачи, хранения (в том числе архивированные) и использования информации,
3) элементы ИТ-инфраструктуры, включая компьютерную технику, библиотеки, архивы, базы данных, сервера, включая физические и виртуальные, каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены защищаемые элементы ИТ-инфраструктуры Общества;
4) процессы, регламенты и процедуры обработки информации в Обществе;
5) сведения, составляющие коммерческую тайну, доступ к которым ограничен собственником информации в соответствии с законодательством Республики Казахстан;
6) персональные данные работников и контрагентов Общества;
7) открытая информация, необходимая для обеспечения нормального функционирования Общества.

3.4. Структура, состав и размещение основных объектов защиты

К основным особенностям информационной среды Общества, относятся:

- объединение в единую систему большого количества разнообразных технических средств обработки и передачи информации;
- значительное расширение сферы использования автоматизированных систем обработки информации, широкое многообразие и повсеместное распространение информационно-управляющих систем в Обществе;
- большое разнообразие решаемых задач и типов обрабатываемых данных, сложные режимы автоматизированной обработки информации с широким совмещением выполнения информационных запросов различных пользователей;
- объединение в единых базах данных информации различного назначения, принадлежности и уровней конфиденциальности;
- наличие большого числа информационных каналов взаимодействия с «внешним миром» (источниками и потребителями информации);
- необходимость обеспечения непрерывности функционирования информационной системы Общества;
- высокая интенсивность информационных потоков.

В этих условиях резко возрастает уязвимость информации и одним из важнейших элементов информационной среды Общества становится корпоративная информационная система, в которой обрабатываются и накапливаются значительные объемы информации, совместно используемой различными пользователями.

Глава 4. Цели и задачи обеспечения информационной безопасности

4.1. Цели защиты.

Основной целью, на достижение которой направлены положения настоящей Политики, является защита субъектов информационных отношений Общества от возможного нанесения им материального, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня операционного и других рисков (риск нанесения урона деловой репутации Общества, правовой риск и т.д.).

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств информации:

- доступности информации для легальных пользователей (устойчивого функционирования информационной системы Общества, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время);
- целостности и аутентичности (подтверждение авторства) информации, хранимой и обрабатываемой в информационной системе Общества и передаваемой по каналам связи;
- конфиденциальности - сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи;

Необходимый уровень доступности, целостности и конфиденциальности информации обеспечивается методами и средствами, соответствующими уровню угроз информационной безопасности.

4.2. Для достижения основной цели защиты и обеспечения указанных свойств информации система обеспечения информационной безопасности Общества должна обеспечивать эффективное решение следующих задач:

1) своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, нарушению нормального функционирования информационной системы Общества;

2) своевременное выявление и устранение уязвимостей активов Общества и тем самым предупреждение возможности нанесения ущерба и нарушения нормального функционирования бизнес-процессов;

3) определение и документирование основных требований и процедур обеспечения информационной безопасности;

4) создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

5) создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;

6) защиту от вмешательства в процесс функционирования информационной системы Общества посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

7) разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам Общества (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа;
8) обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);
9) защиту от несанкционированной модификации используемых в корпоративной информационной системе Общества программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
10) защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
11) обеспечение живучести криптографических средств защиты информации;
12) планирование и оптимизация затрат на обеспечение информационной безопасности Общества.

4.3. Основные пути решения задач системы защиты.

Поставленные основные цели защиты и решение перечисленных выше задач достигаются:

- строгим учетом всех подлежащих защите ресурсов информационной системы Общества (информации, задач, документов, каналов связи, серверов, автоматизированных рабочих мест);
- журналированием действий персонала, осуществляющего обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- полнотой, реальной выполнимостью и непротиворечивостью требований организационно-распорядительных документов Общества по вопросам обеспечения безопасности информации;
- подготовкой (обучением) работников, ответственных за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки;
- наделением каждого пользователя минимально необходимыми для выполнения им своих функциональных обязанностей полномочиями по доступу к информационным ресурсам Общества;
- четким знанием и строгим соблюдением всеми пользователями информационной системы Общества требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого работника, в рамках своих функциональных обязанностей имеющего доступ к информационным ресурсам Общества;
- непрерывным поддержанием необходимого уровня защищенности элементов информационной среды Общества, устранение возможного ущерба при реализации угроз информационной безопасности, в том числе сокращение времени восстановления бизнес-процессов после возможных прерываний;

- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования;
- мониторингом и обработкой событий и инцидентов информационной безопасности;
- эффективным контролем над соблюдением пользователями информационных ресурсов Общества требований по обеспечению безопасности информации;
- юридической защитой интересов Общества при взаимодействии его подразделений с внешними организациями (связанном с обменом информацией) от противоправных действий, как со стороны этих организаций, так и от несанкционированных действий обслуживающего персонала и третьих лиц.

Глава 5. Основные угрозы безопасности информации Общества

5.1. Угрозы безопасности информации и их источники.

Все множество потенциальных угроз безопасности информации по природе их возникновения разделяются на два класса: естественные (объективные) и искусственные (субъективные).

Естественные угрозы - угрозы, вызванные воздействиями на информационную систему и ее компоненты объективных физических процессов техногенного характера или стихийных природных явлений, независящих от человека;

Искусственные угрозы - угрозы, вызванные деятельностью человека. Среди них, исходя из мотивации действий, можно выделить:

- непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п.;
- преднамеренные (умышленные) угрозы, связанные с корыстными, идейными или иными устремлениями людей (злоумышленников).

Источники угроз по отношению к самой информационной системе могут быть как внешними, так и внутренними.

5.2. Наиболее значимыми угрозами безопасности информации Общества (способами нанесения ущерба субъектам информационных отношений) являются:

- нарушение функциональности компонентов информационной системы Общества, блокирование информации, нарушение технологических процессов, срыв своевременного решения задач;
- нарушение целостности (искажение, подмена, уничтожение) информационных, программных и других ресурсов Общества, а также фальсификация (подделка) документов;
- нарушение конфиденциальности (разглашение, утечка) сведений, составляющих служебную или коммерческую тайну, а также персональных данных.

5.3. Пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации.

Работники Общества, зарегистрированные как легальные пользователи информационной системы Общества или обслуживающие ее компоненты, являются внутренними источниками случайных воздействий, т.к. имеют непосредственный доступ к процессам обработки информации и могут совершать непреднамеренные ошибки и нарушения действующих правил, инструкций и регламентов.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз безопасности информации Общества (действия, совершаемые людьми случайно, по незнанию, невнимательности или халатности, из любопытства, но без злого умысла):

- неумышленные действия, приводящие к частичному или полному нарушению функциональности компонентов информационной системы Общества или разрушению информационных или программно-технических ресурсов;
- неосторожные действия, приводящие к разглашению информации ограниченного распространения или делающие ее общедоступной;
- разглашение, передача или утрата атрибутов ограничения доступа (пропусков, идентификационных карточек, ключей, паролей, ключей шифрования и т. п.);
- игнорирование организационных ограничений (установленных правил) при работе с информационными ресурсами;
- проектирование систем, технологий обработки данных, разработка программного обеспечения с возможностями, представляющими опасность для функционирования информационной системы Общества и безопасности информации;
- пересылка данных и документов по ошибочному адресу (устройства);
- ввод ошибочных данных;
- неумышленная порча носителей информации;
- неумышленное повреждение каналов связи;
- неправомерное отключение оборудования или изменение режимов работы устройств или программ;
- заражение компьютеров вирусами;
- несанкционированный запуск технологических программ, способных вызвать потерю работоспособности компонентов Корпоративной информационной системы или осуществляющих необратимые в них изменения (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);
- некомпетентное использование, настройка или неправомерное отключение средств защиты.

5.4. Пути реализации преднамеренных искусственных (субъективных) угроз безопасности информации.

Основные возможные пути умышленной дезорганизации работы, вывода компонентов информационной системы Общества из строя, проникновения в систему и несанкционированного доступа к информации (с корыстными целями, по принуждению, из желания отомстить и т.п.):

- умышленные действия, приводящие к частичному или полному нарушению функциональности компонентов информационной системы Общества или разрушению информационных или программно-технических ресурсов;
- действия по дезорганизации функционирования информационной системы Общества, хищение документов и носителей информации;
- несанкционированное копирование документов и носителей информации, умышленное искажение информации, ввод неверных данных;
- отключение или вывод из строя подсистем обеспечения функционирования информационных систем (электропитания, охлаждения и вентиляции, линий и аппаратуры связи и т.п.);
- перехват данных, передаваемых по каналам связи;
- хищение производственных отходов (распечаток документов, записей, носителей информации и т.п.);
- незаконное получение атрибутов разграничения доступа (агентурным путем, используя халатность пользователей, путем подделки, подбора и т.п.);
- несанкционированный доступ к ресурсам Корпоративной информационной системы с рабочих станций легальных пользователей;
- хищение или вскрытие шифров криптозащиты информации;
- внедрение аппаратных и программных закладок с целью скрытно осуществлять доступ к информационным ресурсам или дезорганизации функционирования компонентов корпоративной информационной системы Общества;
- незаконное использование оборудования, программных средств или информационных ресурсов, нарушающее права третьих лиц;
- применение подслушивающих устройств, дистанционная фото- и видео съемка для несанкционированного съема информации;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на технические средства, непосредственно не участвующие в информационном обмене (сети питания).

5.5. Пути реализации основных естественных угроз безопасности информации:

- выход из строя оборудования информационных систем и оборудования обеспечения его функционирования;

- выход из строя или невозможность использования линий связи;
- пожары, наводнения и другие стихийные бедствия.

5.6. Система обеспечения информационной безопасности Общества должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

- некомпетентный (невнимательный) пользователь - работник Общества (или подразделения другой организации, являющийся легальным пользователем информационной системы Общества), который может предпринимать попытки выполнения запрещенных действий, доступа к защищаемым ресурсам информационной системы с превышением своих полномочий, ввода некорректных данных, нарушения правил и регламентов работы с информацией и т.п., действуя по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (предоставленные) средства;
- любитель - работник Общества (или подразделения другой организации, являющийся зарегистрированным пользователем информационной системы Общества), пытающийся нарушить систему защиты без корыстных целей или злого умысла или для самоутверждения. Для преодоления системы защиты и совершения запрещенных действий он может использовать различные методы получения дополнительных полномочий доступа к ресурсам, недостатки в построении системы защиты и доступные ему штатные средства (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого, он может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства, самостоятельно разработанные программы или стандартные дополнительные технические средства;
- внутренний злоумышленник - работник Общества (или подразделения другого ведомства, зарегистрированный как пользователь системы), действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися работниками Общества. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Общества;

- внешний злоумышленник - постороннее лицо, действующее целенаправленно из корыстных интересов, мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор методов и средств взлома системы защиты, включая агентурные методы, пассивные средства (технические средства перехвата), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий, как изнутри, так и извне Общества.

Глава 6. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов

6.1. Все меры обеспечения безопасности информационной системы Общества подразделяются на:

6.1.1. Правовые (законодательные) меры защиты.

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил. Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом информационной системы Общества.

6.1.2. Технологические меры защиты.

К данному виду мер защиты относятся технологические решения и приемы, основанные на использовании некоторых видов избыточности (структурной, функциональной, информационной, временной и т.п.) и направленные на уменьшение возможности совершения работниками ошибок и нарушений в рамках предоставленных им прав и полномочий. Примером таких мер является использование процедур двойного ввода ответственной информации, инициализации ответственных операций только при наличии согласования нескольких лиц, процедур проверки реквизитов исходящих и входящих сообщений и т.п.

6.1.3. Организационные (административные) меры защиты.

Организационные (административные) меры защиты - это меры организационного характера, регламентирующие процессы функционирования системы обработки данных, использование ее ресурсов, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

6.2. Регламентация допуска работников к использованию информационных ресурсов.

В рамках разрешительной системы допуска устанавливается: кто, кому, какую информацию и для какого вида доступа может предоставить и при каких условиях. Допуск пользователей к работе с информационной системой Общества и доступ к ее ресурсам должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться установленным порядком, согласно, регламента предоставления доступа пользователей.

Основными пользователями информации в Корпоративной информационной системе являются работники структурных подразделений Общества. Уровень полномочий каждого пользователя определяется индивидуально. Каждый работник пользуется только предписанными ему правами по отношению к информации, с которой ему необходима работа в соответствии с должностными обязанностями. Расширение прав доступа и предоставление доступа к дополнительным информационных ресурсам, в обязательном порядке, должно согласовываться с подразделением Общества, ответственным за информационное сопровождение данного ресурса.

6.3. Регламентация процессов обслуживания и осуществления модификации аппаратных и программных ресурсов.

Подлежащие защите ресурсы системы (документы, задачи, сервера, программы) подлежат строгому учету (на основе использования соответствующих формуляров или специализированных баз данных).

В целях поддержания режима информационной безопасности аппаратно-программная конфигурация автоматизированных рабочих мест работников Общества, с которых возможен доступ к ресурсам корпоративной информационной системы, должна соответствовать кругу возложенных на данных пользователей функциональных обязанностей. Все неиспользуемые в работе устройства ввода-вывода информации на рабочих местах работников, работающих с конфиденциальной информацией, должны быть по возможности отключены, не нужные для работы программные средства и данные с дисков также должны быть удалены. Дополнительные устройства обмена информацией могут использоваться только в исключительных случаях и только в качестве временного средства. Установка подобных устройств должна согласовываться с подразделениями обеспечения информационной безопасности Общества.

В компонентах корпоративной информационной системы и на рабочих местах пользователей должны устанавливаться и использоваться программные средства, только полученные от Департамента информационных технологий. Использование программного обеспечения, не прошедшего проверку и не учтенного в Обществе, должно быть запрещено.

Для решения специальных задач по оценке защищенности информационной сети Общества и построении системы защиты информации в сети Общества может применяться специальное программное обеспечение.

6.4. Обеспечение и контроль физической целостности (неизменности конфигурации) аппаратных ресурсов.

Оборудование корпоративной информационной системы, используемое для доступа к конфиденциальной информации, к которому доступ обслуживающего персонала в процессе эксплуатации не требуется, после наладочных, ремонтных и

иных работ, связанных с доступом к его компонентам, должно закрываться и опечатываться (пломбироваться). Повседневный контроль за целостностью и соответствием печатей (пломб) должен осуществляться пользователями оборудования, периодический контроль – Службой безопасности Общества.

6.5. Пользователи информационной системы Общества, а также руководящий и обслуживающий персонал должны быть ознакомлены со своим уровнем полномочий, а также организационно-распорядительной, нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки информации в Обществе.

Глава 7. Подразделения обеспечения информационной безопасности

7.1. Непосредственная организация работы по обеспечению информационной безопасности возлагается на Службу безопасности и Департамент информационных технологий Общества.

7.2. Основные функции подразделений обеспечения информационной безопасности:

- проведение в жизнь политики информационной безопасности Общества;
- организация мероприятий и координация работ всех подразделений Общества по комплексной защите информации;
- анализ текущего состояния обеспечения безопасности информации;
- разрабатывание нормативных документов, касающихся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы Общества;
- формирование требований информационной безопасности и к системе защиты в процессе создания и дальнейшего развития существующих компонентов информационной системы Общества;
- участие в проектировании систем и программ защиты, их испытаниях и приемке в эксплуатацию;
- обеспечение функционирования установленных систем защиты информации, включая управление криптографическими системами;
- распределение между пользователями необходимых атрибутов доступа к ресурсам информационной системы Общества;
- наблюдение за функционированием системы защиты и ее элементов;
- проверка надежности функционирования системы защиты;
- разработка мер нейтрализации моделей возможных атак;
- обучение пользователей и обслуживающего персонала правилам безопасной обработки информации;
- оказание методической помощи работникам Общества в вопросах обеспечения информационной безопасности;
- контроль за действиями администраторов баз данных, серверов и сетевых устройств;
- контроль за соблюдением пользователями установленных правил обращения с информацией;

- контроль и оценка эффективности принятых мер и применяемых средств защиты информации;
- принятие мер при попытках несанкционированного доступа к информационным ресурсам и компонентам системы или при нарушениях правил функционирования системы защиты;
- сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;
- проведение служебных проверок и расследований по фактам нарушения требований информационной безопасности.

7.3. Для решения задач, возложенных на них задач подразделения обеспечения информационной безопасности имеют право:

- получать информацию от пользователей информационной системы Общества по любым аспектам информационной безопасности;
- прекращать обработку информации при наличии непосредственной угрозы для нее;
- участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
- участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
- контролировать деятельность пользователей информационной системы Общества по вопросам обеспечения информационной безопасности;
- инициировать привлечение к ответственности работников, допускающих нарушения требований информационной безопасности.

Глава 8. Ответственность за нарушения требований информационной безопасности

Работники Общества несут персональную ответственность за нарушения установленного порядка обработки информации, правил хранения, использования и передачи находящихся в их распоряжении защищаемых ресурсов системы. Каждый работник при приеме на работу должен подписывать обязательство о соблюдении и ответственности за нарушение установленных требований по сохранению служебной и коммерческой тайны, а также правил работы с информацией в Обществе. Мера ответственности работников Общества за действия, совершенные в нарушение установленных правил и требований информационной безопасности, определяется нанесенным ущербом, наличием злого умысла и другими факторами по усмотрению руководства Общества.

Глава 9. Организационно-правовой режим обеспечения информационной безопасности

Внедрение в Обществе организационно-правового режима обеспечения информационной безопасности предусматривает разработку и утверждение необходимых нормативных документов:

- определенных законодательством Республики Казахстан касательно информационной безопасности и обязательных для исполнения;
- касательно сведений, составляющих коммерческую тайну Общества (положение о коммерческой тайне, перечень сведений, составляющих коммерческую и служебную тайну Общества);
- приказы и распоряжения руководства Общества касательно режима безопасности.

Глава 10. Заключительные положения

10.1. Вопросы, не урегулированные настоящей Политикой, регулируются в соответствии с законодательством Республики Казахстан.

10.2. В случае возникновения противоречий Политики требованиям законодательства Республики Казахстан, Политика подлежит применению в части не противоречащей законодательным и нормативным правовым актам Республики Казахстан.

10.3. Требования Политики распространяются на всех работников Общества. Выполнение требований Политики работниками подразделений обеспечивается руководителями подразделений и курирующими руководителями.

10.4. Настоящая Политика вступает в силу с даты утверждения Правлением Общества.

10.5. Изменения и дополнения в настоящую Политику вносятся по решению Правления Общества.

ЛИСТ СОГЛАСОВАНИЯ

к Политике информационной безопасности АО «СПК «Алматы»

Должность	ФИО	Подпись	Дата
Заместитель председателя Правления	Габдуллин А.Ж.		19.07.23г
Заместитель председателя Правления	Касенова З.А.		19.07.23г
Заместитель председателя Правления	Алдажаров Е.К.		19.07.23
Управляющий директор	Садыков М.Ж.		19.07.23г.
Руководитель Службы безопасности	Самаков Ч.К.		19.07.23
Директор Департамента риск-менеджмента	Рябов А.Н.		19.07.23
Директор Департамента правового обеспечения	Менсеитов Р.С.		19.07.23
Директор Департамента стратегии и корпоративного развития	Ибраева Ш.Д.		19.07.23
Директор Департамента информационных технологий	Чеботов Д.А.		19.07.23

Выписка из протокола
Заседания Правления акционерного общества
«Социально-предпринимательская корпорация «Алматы»

г. Алматы **37** **19.07.2023**

Место и время проведения заседания Правления:
г.Алматы, Бостандыкский район, Байзакова, 303, 10:20 часов

Председатель Правления:	Шамшин А. Н.
Члены Правления:	
Заместитель Председателя Правления	Габдуллин А.Ж.
Заместитель Председателя Правления	Касенова З. А.
Заместитель Председателя Правления	Алдажаров Е.К.
Секретарь Правления:	Усенбаев Д.
Приглашенные участники заседания:	
Управляющий директор	Садыков М.Ж.
Директор департамента правового обеспечения	Менсеитов Р.С.
Руководитель секритариата	Кажденов Н.Е.

Согласно Положения о Правлении АО «Социально - предпринимательская корпорация «Алматы» необходимый кворум для проведения заседания Правления имеется.

1. Вопрос: Об утверждении Политики информационной безопасности АО «СПК «Алматы».

Докладчик по вопросу: Руководитель Службы безопасности Самаков Ч.К.

По итогам голосования принято следующее решение:
Утвердить Политику информационной безопасности АО «СПК «Алматы», согласно приложению №1 к настоящему протоколу.

Секретарь Правления **Усенбаев Д.**