1. Общие положения ……………………………………………………………………. 2
2. Список терминов и определений …………………………………………………... 3
3. Описание объекта защиты…………………………………………………………… 4
4. Цели и задачи деятельности по обеспечению

информационной безопасности ……………………………………………………. 5

5. Угрозы информационной безопасности…………………………………………….5

6. Модель нарушения информационной безопасности……………………………..6

7. Основные положения по обеспечению информационной безопасности……..7

8. Организационная основа деятельности по

обеспечению информационной безопасности…………………………………….10

9. Ответственность за соблюдение положений Политики………………………….12

10. Контроль за соблюдением положений Политики………………………………....12

11. Заключительные положения………………………………………………………….12

**1. Общие положения**

1.1. Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности, требованиями нормативных актов Центрального Компании Российской Федерации, федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается в том числе на:

Доктрине информационной безопасности Российской Федерации (от 09.09.2000 Пр-1895);

1.2. Настоящая Политика является документом, доступным любому сотруднику Компании и пользователю его ресурсов, и представляет собой официально принятую руководством «Солнышко» (Общество с ограниченной ответственностью) (далее – Компания) систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе систематизированного изложения целей, процессов и процедур информационной безопасности Компании.

1.3. Руководство Компании осознает важность и необходимость развития и совершенствования мер и средств обеспечения информационной безопасности. Соблюдение требований информационной безопасности позволит создать конкурентные преимущества Компании, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

1.4. Требования информационной безопасности, которые предъявляются Компанией, соответствуют интересам (целям) деятельности Компании и предназначены для снижения рисков, связанных с информационной безопасностью, до приемлемого уровня. Факторы рисков в информационной сфере Компании имеют отношение к его корпоративному управлению (менеджменту), организации и реализации бизнес-процессов, взаимоотношениям с контрагентами и клиентами, внутрихозяйственной деятельности. Факторы рисков в информационной сфере Компании составляют значимую часть операционных рисков Компании, а также имеют отношение и к иным рискам основной и управленческой деятельности Компании.

1.5. Стратегия Компании в области обеспечения информационной безопасности и защиты информации наряду с прочим включает выполнение в практической деятельности требований:

российского законодательства в области безопасности, безопасности информационных технологий и защиты информации, безопасности персональных данных и других правовых актов;

нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения физической безопасности и технической защиты информации, противодействия техническим разведкам и обеспечения информационной безопасности и приватности;

нормативных актов Компании России и стандартов Компании России по обеспечению информационной безопасности из комплекса стандартов «СТО БР ИББС»;

1.6. Необходимые требования обеспечения информационной безопасности Компании должны неукоснительно соблюдаться персоналом Компании и другими сторонами как это определяется положениями внутренних нормативных документов Компании, а также требованиями договоров и соглашений, стороной которых является Компания.

1.7. Настоящая Политика распространяется на бизнес - процессы Компании и обязательна для применения всеми сотрудниками и руководством Компании, а также пользователями его информационных ресурсов.

1.8. Положения настоящей Политики должны быть учтены при разработке политик информационной безопасности в дочерних и аффилированных организациях.

1.9. Документами, детализирующими положения корпоративной Политики применительно к одной или нескольким областям ИБ, видам и технологиям деятельности Компании, являются частные политики по обеспечению ИБ (далее – Частные политики), которые являются документами по ИБ второго уровня, оформляются как отдельные внутренние нормативные документы Компании, разрабатываются и согласовываются в соответствии с установленным в Компании порядком, утверждаются Куратором.

**2. Список терминов и определений**

2.1. **Бизнес-процесс** – последовательность технологически связанных операций по предоставлению продуктов и/или осуществлению конкретного вида обеспечивающей деятельности Компании.

2.2. **Информационная безопасность Компании (ИБ)** – в настоящей Политике состояние защищенности технологических и бизнес - процессов Компании, объединяющих в своем составе сотрудников Компании, технические и программные средства обработки информации, информацию в условиях угроз в информационной сфере.

2.3. **Информационная система Компании** – совокупность программно-аппаратных комплексов Компании, применяемых для обеспечения бизнес - процессов Компании.

2.4. **Инцидент информационной безопасности** – это появление одного или нескольких нежелательных рисковых событий информационной безопасности, с которыми связана значительная вероятность нарушения конфиденциальности, целостности или доступности информационных активов и инфраструктуры и создания угрозы информационной безопасности.

2.5. **ИТ-блок** – совокупность самостоятельных структурных подразделений Компании, ответственных за развитие, эксплуатацию и сопровождение информационных систем.

2.6. **Конфиденциальная информация (далее – КИ)** – информация, в отношении которой Компанией установлен режим конфиденциальности.

2.7. **Куратор** – заместитель Председателя Правления Компании, курирующий вопросы безопасности Компании, в том числе вопросы информационной безопасности.

2.8. **Модель угроз** – описательное представление свойств или характеристик угроз безопасности информации.

2.9. **Модель нарушителя** – описательное представление опыта, знаний, доступных ресурсов возможных нарушителей ИБ, необходимых им для реализации угрозы ИБ, и возможной мотивации действий.

2.10. **Ответственное подразделение** – Служба (департамент) безопасности. Основные функции в указанной сфере – внедрение настоящей Политики, разработка, внедрение и поддержка систем обеспечения информационной безопасности.

2.11. **Пользователь информационной системы** - физическое лицо, обладающее возможностью доступа к информационной системе Компании.

2.12.**Режим конфиденциальности информации** – организационно-технические мероприятия по защите информации, позволяющие обладателю КИ при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду, и реализующие меры по охране КИ, включающие в себя:

* определение перечня информации, составляющей КИ в соответствии с «Перечнем информации, в отношении которой ГПБ (ООО) установлен режим конфиденциальности», утвержденным приказом от 27.05.2011 № 47);
* ограничение доступа к КИ путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
* учет лиц, получивших доступ к КИ, и (или) лиц, которым такая информация была предоставлена или передана;
* регулирование отношений по использованию КИ работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров и соглашений.

2.13. **Рисковое событие информационной безопасности** – это событие, обусловленное операционным риском, повлекшее или способное повлечь за собой потери Компании и произошедшее по причине ошибочности или сбоя процессов, действий людей и систем, а также по причине внешних событий.

2.14. **Угроза информационной безопасности** – операционный риск, влияющий на нарушение одного (или нескольких) свойств информации – целостности, конфиденциальности, доступности объектов защиты.

**3. Описание объекта защиты**

Основными объектами защиты системы информационной безопасности в Компании являются:

* информационные ресурсы, содержащие коммерческую тайну, персональные данные физических лиц, сведения ограниченного распространения, а также открыто распространяемая информация, необходимая для работы Компании, независимо от формы и вида ее представления;
* информационные ресурсы, содержащие конфиденциальную информацию, включая персональные данные физических лиц, а также открыто распространяемая информация, необходимая для работы Компании, независимо от формы и вида ее представления;
* сотрудники Компании, являющиеся разработчиками и пользователями информационных систем Компании;
* информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

**4. Цели и задачи деятельности по обеспечению информационной безопасности**

Целью деятельности по обеспечению информационной безопасности Компании является снижение угроз информационной безопасности до приемлемого для Компании уровня. Основные задачи деятельности по обеспечению информационной безопасности Компании:

* выявление потенциальных угроз информационной безопасности и уязвимостей объектов защиты;
* предотвращение инцидентов информационной безопасности;
* исключение либо минимизация выявленных угроз.

**5. Угрозы информационной безопасности**

Все множество потенциальных угроз безопасности информации делится на три класса по природе их возникновения: антропогенные, техногенные и естественные (природные).

5.1. Возникновение антропогенных угроз обусловлено деятельностью человека. Среди них можно выделить угрозы, возникающие вследствие как непреднамеренных (неумышленных) действий: угрозы, вызванные ошибками в проектировании информационной системы и ее элементов, ошибками в действиях персонала и т.п., так и угрозы, возникающие в силу умышленных действий, связанные с корыстными, идейными или иными устремлениями людей. К антропогенным угрозам относятся угрозы, связанные с нестабильностью и противоречивостью требований регуляторов деятельности Компании и контрольных органов, с действиями в руководстве и управлении (менеджменте), неадекватными целям и сложившимся условиям, с потребляемыми услугами, с человеческим фактором.

5.2. Возникновение техногенных угроз обусловлено воздействиями на объект угрозы объективных физических процессов техногенного характера, технического состояния окружения объекта угрозы или его самого, не обусловленных напрямую деятельностью человека. К техногенным угрозам могут быть отнесены сбои, в том числе в работе, или разрушение систем, созданных человеком.

5.3. Возникновение естественных (природных) угроз обусловлено воздействиями на объект угрозы объективных физических процессов природного характера, стихийных природных явлений, состояний физической среды, не обусловленных напрямую деятельностью человека.

**6. Модель нарушителя информационной безопасности**

По отношению к Компании нарушители могут быть разделены на внешних и внутренних нарушителей.

6.1. Внутренние нарушители. В качестве потенциальных внутренних нарушителей Компанией рассматриваются:

* зарегистрированные пользователи информационных систем Компании;
* сотрудники Компании, не являющиеся зарегистрированными пользователями и не допущенные к ресурсам информационных систем Компании, но имеющие доступ в здания и помещения;
* персонал, обслуживающий технические средства корпоративной информационной системы Компании;
* сотрудники самостоятельных структурных подразделений Компании, задействованные в разработке и сопровождении программного обеспечения;
* сотрудники самостоятельных структурных подразделений, обеспечивающие безопасность Компании;
* руководители различных уровней.

6.2. Внешние нарушители. В качестве потенциальных внешних нарушителей Компанией рассматриваются:

* бывшие сотрудники Компании;
* представители организаций, взаимодействующих по вопросам технического обеспечения Компании;
* клиенты Компании;
* посетители зданий и помещений Компании;
* конкурирующие с Компанией кредитные организации;
* члены преступных организаций, сотрудники спецслужб или лица, действующие по их заданию;
* лица, случайно или умышленно проникшие в корпоративную информационную систему Компании из внешних телекоммуникационных сетей (хакеры).

6.3. В отношении внутренних и внешних нарушителей принимаются следующие ограничения и предположения о характере их возможных действий:

* нарушитель скрывает свои несанкционированные действия от других сотрудников Компании;
* несанкционированные действия нарушителя могут быть следствием ошибок пользователей, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;
* в своей деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и информационные системы, адекватные финансовые средства для подкупа персонала, шантаж, методы социальной инженерии и другие средства и методы для достижения стоящих перед ним целей;
* внешний нарушитель может действовать в сговоре с внутренним нарушителем.

**7. Основные положения по обеспечению информационной безопасности**

7.1. Требования об обеспечении информационной безопасности Компании обязательны к соблюдению всеми работниками Компании и пользователями информационных систем.

7.2. Руководство Компании приветствует и поощряет в установленном порядке деятельность работников Компании и пользователей информационных систем по обеспечению информационной безопасности.

7.3. Неисполнение или некачественное исполнение сотрудниками Компании и пользователей информационных систем обязанностей по обеспечению информационной безопасности может повлечь лишение доступа к информационным системам, а также применение к виновным административных мер воздействия, степень которых определяется установленным в Компании порядком либо требованиями действующего законодательства.

7.4. Стратегия Компании в части противодействия угрозам информационной безопасности заключается в сбалансированной реализации взаимодополняющих мер по обеспечению безопасности: от организационных мер на уровне руководства Компании, до специализированных мер информационной безопасности по каждому выявленному в Компании риску, основанных на оценке рисков информационной безопасности.

7.5. С целью поддержки заданного уровня защищенности Компания придерживается процессного подхода в построении системы менеджмента информационной безопасности. Система менеджмента информационной безопасности Компании основывается на осуществлении следующих основных процессов (планирование, реализация и эксплуатация защитных мер, проверка (мониторинг и анализ), совершенствование) соответствующих требованиям стандарта Компании России СТО БР ИББС–1.0 и положениям международных стандартов по обеспечению информационной безопасности. Реализация этих процессов осуществляется в виде непрерывного цикла – «планирование – реализация – проверка – совершенствование – планирование – …», направленного на постоянное совершенствование деятельности по обеспечению информационной безопасности Компании и повышение ее эффективности. На всех этапах жизненного цикла управление информационной безопасностью Компании осуществляется с соблюдением нормативных документов, определяющих процессы управления операционными рисками Компании.

7.6. При планировании мероприятий по обеспечению информационной безопасности в Компании осуществляются:

7.6.1. Определение и распределение ролей персонала Компании, связанного с обеспечением информационной безопасности (ролей информационной безопасности).

7.6.2. Оценка важности информационных активов с учетом потребности в обеспечении их свойств с точки зрения информационной безопасности.

7.6.3. Менеджмент рисков информационной безопасности, включающий:

* анализ влияния на информационную безопасность Компании применяемых в деятельности Компании технологий, а также внешних по отношению к Компании событий;
* выявление проблем обеспечения информационной безопасности, анализ причин их возникновения и прогнозирование их развития;
* определение моделей угроз информационной безопасности;
* выявление, анализ и оценка значимых для Компании угроз информационной безопасности;
* выявление возможных негативных последствий для Компании, наступающих в результате проявления факторов риска информационной безопасности, в том числе связанных с нарушением свойств безопасности информационных активов Компании;
* идентификацию и анализ рисковых событий информационной безопасности;
* оценку величины рисков информационной безопасности и определение среди них рисков, неприемлемых для Компании;
* обработку результатов оценки рисков информационной безопасности, базирующейся на методах управления операционными рисками, определенных в Компании ;
* оптимизацию рисков информационной безопасности за счет выбора и применения защитных мер, противодействующих проявлениям факторов риска и минимизирующих возможные негативные последствия для Компании в случае наступления рисковых событий;
* оценку влияния защитных мер на цели основной деятельности Компании;
* оценку затрат на реализацию защитных мер;
* рассмотрение и оценку различных вариантов решения задач по обеспечению информационной безопасности;
* разработку планов управления рисками, предусматривающих различные защитные меры и варианты их применения, и выбор из них такого, реализация которого максимально положительно скажется на целях основной деятельности Компании и будет оптимальна с точки зрения произведенных затрат и ожидаемого эффекта;
* документальное оформление целей и задач обеспечения информационной безопасности Компании, поддержка в актуальном состоянии нормативно – методического обеспечения деятельности в сфере информационной безопасности.

7.7. В рамках реализации деятельности по обеспечению информационной безопасности в Компании осуществляются:

7.7.1. Менеджмент инцидентов информационной безопасности, включающий:

* сбор информации о событиях информационной безопасности;
* выявление и анализ инцидентов информационной безопасности;
* расследование инцидентов информационной безопасности;
* оперативное реагирование на инцидент информационной безопасности;
* минимизация негативных последствий инцидентов информационной безопасности;
* оперативное доведение до руководства Компании информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
* выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
* пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
* повышение уровня знаний персонала Компании в вопросах обеспечения информационной безопасности;
* обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Компании и информации, обрабатываемой в них;
* применение средств криптографической защиты информации;
* обеспечение бесперебойной работы автоматизированных систем и сетей связи;
* обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
* применение средств защиты от вредоносных программ;
* обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем Компании, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
* обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
* контроль доступа в здания и помещения Компании.

7.7.2. Обеспечение защиты информации от утечки по техническим каналам, включающее:

* применение мер и технических средств, снижающих вероятность несанкционированного получения информации в устной форме - пассивная защита;
* применение мер и технических средств, создающих помехи при несанкционированном получении информации - активная защита;
* применение мер и технических средств, позволяющих выявлять каналы несанкционированного получения информации - поиск.

7.8. В целях проверки деятельности по обеспечению информационной безопасности в Компании осуществляются:

* контроль правильности реализации и эксплуатации защитных мер;
* контроль изменений конфигурации систем и подсистем Компании;
* мониторинг факторов рисков3 и соответствующий их пересмотр;
* контроль реализации и исполнения требований сотрудниками Компании действующих внутренних нормативных документов по обеспечению информационной безопасности Компании;
* контроль деятельности сотрудников и других пользователей информационных систем Компании, направленный на выявление и предотвращение конфликтов интересов.

7.9. В целях совершенствования деятельности по обеспечению информационной безопасности в Компании осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Компании).

**8. Организационная основа деятельности по обеспечению информационной безопасности**

8.1. В целях выполнения задач по обеспечению информационной безопасности Компании, в соответствии с рекомендациями международных и российских стандартов по безопасности в Компании должны быть определены следующие роли:

* Куратор;
* Ответственное подразделение;
* Сотрудник Компании.

При необходимости могут быть определены и другие роли по информационной безопасности.

8.2. Оперативная деятельность и планирование деятельности по обеспечению информационной безопасности Компании осуществляются и координируются Ответственным подразделением. Задачами Ответственного подразделения являются:

* установление потребностей Компании в применении мер обеспечения информационной безопасности, определяемых как внутренними корпоративными требованиями, так и требованиями нормативных актов;
* соблюдение действующего федерального законодательства, нормативных актов федеральных органов исполнительной власти, уполномоченных в области обеспечения безопасности и противодействия техническим разведкам и технической защиты информации, нормативных актов Компании России и стандартов Компании России по обеспечению информационной безопасности, нормативных актов по обеспечению информационной безопасности, приватности и неразглашению, принятых регуляторами рынков, на которых представлены интересы и бизнес Компании;
* разработка и пересмотр внутренних нормативных документов по обеспечению информационной безопасности Компании, включая планы, политики, положения, регламенты, инструкции, методики, перечни сведений и иные виды внутренних нормативных документов;
* осуществление контроля актуальности и непротиворечивости внутренних нормативных документов (политик, планов, методик и т.д.), затрагивающих вопросы информационной безопасности Компании;
* обучение, контроль и непосредственная работа с персоналом Компании в области обеспечения информационной безопасности;
* планирование применения, участие в поставке и эксплуатации средств обеспечения информационной безопасности на объекты и системы в Компании;
* выявление и предотвращение реализации угроз информационной безопасности;
* выявление и реагирование на инциденты информационной безопасности;
* информирование в установленном порядке ответственных лиц об угрозах и рисковых событиях информационной безопасности;
* прогнозирование и предупреждение инцидентов информационной безопасности;
* пресечение несанкционированных действий нарушителей информационной безопасности;
* поддержка базы инцидентов информационной безопасности, анализ, разработка оптимальных процедур реагирования на инциденты и обучение персонала;
* типизация решений по применению мер и средств обеспечения информационной безопасности и распространение типовых решений на филиалы и представительства Компании;
* обеспечение эксплуатации средств и механизмов обеспечения информационной безопасности;
* мониторинг и оценка информационной безопасности, включая оценку полноты и достаточности защитных мер и видов деятельности по обеспечению информационной безопасности Компании;
* контроль обеспечения информационной безопасности Компании, в том числе, и на основе информации об инцидентах информационной безопасности, результатах мониторинга, оценки и аудита информационной безопасности;
* информирование руководства Компании и руководителей его самостоятельных структурных подразделений Компании об угрозах информационной безопасности, влияющих на деятельность Компании.

8.3. Ответственное подразделение может создавать оперативные группы для проведения расследований инцидентов информационной безопасности, возглавляемые сотрудником Ответственного подразделения, и может, при наличии обоснованной необходимости по согласованию с руководителями соответствующих подразделений, привлекать для работы в них сотрудников других самостоятельных структурных подразделений Компании на основе совмещения работы в группе со своими основными должностными обязанностями.

8.4. Финансирование работ по реализации положений настоящей Политики осуществляется как в рамках целевого бюджета Ответственного подразделения Компании, так и в рамках бюджетов бизнес - подразделений и подразделений ИТ-блока.

8.5. Основными функциями Куратора в вопросах информационной безопасности являются:

назначение ответственных лиц в области ИБ, координация и внедрение информационной безопасности в Компании.

8.6. Основными задачами работников Компании при выполнении возложенных на них обязанностей и в рамках их участия в оперативной деятельности по обеспечению информационной безопасности Компании являются:

* соблюдение требований информационной безопасности, устанавливаемых нормативными документами Компании;
* выявление и предотвращение реализации угроз информационной безопасности в пределах своей компетенции;
* выявление и реагирование на инциденты информационной безопасности;
* информирование в установленном порядке ответственных лиц о выявленных угрозах и рисковых событиях информационной безопасности;
* прогнозирование и предупреждение инцидентов информационной безопасности в пределах своей компетенции;
* мониторинг и оценка информационной безопасности в рамках своего участка работы (рабочего места, структурного подразделения) и в пределах своей компетенции;
* информирование своего руководства и Ответственного подразделения о выявленной угрозе в информационной среде Компании.

**9. Ответственность за соблюдение положений Политики**

Общее руководство обеспечением информационной безопасности Компании осуществляет Куратор. Ответственность за поддержание положений настоящей политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы системы менеджмента информационной безопасности Компании лежит на руководстве Ответственного подразделения. Ответственность работников Компании за невыполнение настоящей Политики определяется соответствующими положениями, включаемыми в договоры с работниками Компании, а также положениями внутренних нормативных документов Компании.

**10. Контроль за соблюдением положений Политики**

Общий контроль состояния информационной безопасности Компании осуществляется Куратором. Текущий контроль соблюдения настоящей Политики осуществляет Ответственное подразделение. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов информационной безопасности Компании, по результатам оценки информационной безопасности, а также в рамках иных контрольных мероприятий. Департамент внутреннего контроля осуществляет контроль соблюдения настоящей Политики на основе проведения внутреннего аудита информационной безопасности.

**11. Заключительные положения**

11.1. Требования настоящей Политики могут развиваться другим внутренними нормативными документами Компании, которые дополняют и уточняют ее.

11.2. В случае изменения действующего законодательства и иных нормативных актов, а также Устава Компании настоящая Политика и изменения к ней применяются в части, не противоречащей вновь принятым законодательным и иным нормативным актам, а также Уставу Компании. В этом случае Ответственное подразделение обязано незамедлительно инициировать внесение соответствующих изменений.

11.3. Внесение изменений в настоящую Политику осуществляется на периодической и внеплановой основе:

* периодическое внесение изменений в настоящую Политику должно осуществляться не реже одного раза в 24 месяца;
* внеплановое внесение изменений в настоящую Политику может производиться по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

11.4. Ответственным за внесение изменений в настоящую Политику является руководитель Ответственного подразделения.