Политика ИБ «Солнышко»

1. **Общие положения**
   1. Политика информационной безопасности компании ООО «Солнышко» определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, процедур, практических приемов, требований и руководящих принципов в области информационной безопасности которыми руководствуются работники компании при осуществлении своей деятельности.
   2. Настоящая Политика доступна каждому сотруднику и клиенту компании. И представляет собой систему взглядов на проблему информационной защиты, и устанавливает систему принципов по работе с информационной безопасностью.
   3. Руководство компании понимает важность и необходимость мер по обеспечению информационной безопасности для развития компании и ее технологий. Такой подход позволит компании создать конкурентные преимущества, обеспечить финансовую стабильность, рентабельность в соответствии с законами и правовыми документами.
   4. Требования информационной безопасности, предъявляемые компанией, соответствуют их интересам, а также снижают долю рисков защиты информации. Факторы рисков в информационной сфере имеют отношение к ее корпоративному управлению, к работе и взаимодействию с клиентами, заказчиками, а также играют важную роль в организации и реализации бизнес-проектов.
   5. Необходимые требования обеспечения информационной безопасности должны соблюдаться сотрудниками, а также другими сторонами.
   6. Положения настоящей политики должны быть уточнены при разработке ротик ИБ в дочерних компаниях или филиалах
   7. Настоящая политика ИБ распространяется на бизнес-процессы предприятия, также ее обязаны соблюдать сотрудники, и пользователи информационных ресурсов
   8. Настоящая Политика в соответствии со всеми правовыми документами и законами является документом по ИБ первого уровня
   9. Документами детализирующими настоящую политику ИБ являются частные политики ИБ, которые выступают в роли документов по ИБ второго уровня.

## **Термины и определения**

* **Бизнес-процесс** — это совокупность взаимосвязанных мероприятий или работ, направленных на создание определённого продукта или услуги для потребителей (под "потребителем" может пониматься в т.ч. внутренний корпоративный субъект, заинтересованный в получении результата процесса, например, бизнес-процесс по формированию и сдаче бухгалтерской отчётности гос.органам.)
* **Риск** — возможность возникновения финансовых потерь (убытков), незапланированных расходов или возможность снижения планируемых доходов.
* **Операционные риски** — это риски, связанные с финансово-экономической деятельностью (без учета рыночных и кредитных рисков), потери по которым связаны с результатами некомпетентного управления человеческими, технологическими факторами или внешними событиями.
* **Служба автоматизаци**и — Департамент ИТ и отдельные сотрудники, ответственные за обеспечение IT-сервиса (в том числе и организации, выполняющие данные работы по договору).
* **Автоматизированная система обработки информации (АС)** — организационно-техническая система, представляющая собой совокупность следующих взаимосвязанных компонентов: технических средств обработки и передачи данных (средств вычислительной техники и связи), методов и алгоритмов обработки в виде соответствующего программного обеспечения, массивов (наборов, баз) данных на различных носителях, персонала и пользователей, объединенных по организационно-структурному, тематическому, технологическому или другим признакам для выполнения автоматизированной обработки данных с целью удовлетворения информационных потребностей государственных органов, коммерческих или некоммерческих организаций (юридических лиц), граждан (физических лиц) и иных потребителей информации.
* **Информационные средства** — средства, предназначенные для хранения, обработки и передачи компьютерной информации, а именно: компьютеры и комплексы, терминалы доступа к ним, оборудование локальных вычислительных сетей и узлов связи, специальное оборудование на основе компьютеров, криптографическое оборудование.
* **Информационный актив** — различные виды информации (платежной, финансово-аналитической, служебной, управляющей, справочной и пр.) на всех этапах ее жизненного цикла, обеспечивающей деятельность и представляющей ценность с точки зрения достижения поставленных бизнес-целей.
* **Компьютерная платфо́рма** — в общем смысле, это любая существующая среда выполнения, в которой должен выполняться вновь разрабатываемый фрагмент программного обеспечения или объектный модуль с учётом накладываемых этой средой ограничений и предоставляемых возможностей.
* **Владелец информационного актива** — структурное подразделение, отдел, служба, реализующее полномочия владения, пользования и распоряжения информацией в соответствии со своими функциями и задачами. Владелец информационного актива определяется на этапе его создания.
* **Инцидент информационной безопасности** — действительное, предпринимаемое или вероятное нарушение информационной безопасности. Нарушение может быть вызвано ошибками персонала, неправильным функционированием технических средств, природными факторами, преднамеренными злоумышленными действиями, приводящими к нарушению доступности, целостности, конфиденциальности информации.
* **Модель** **угроз** (безопасности информации) – физическое, математическое, описательное представление свойств или характеристик **угроз** безопасности информации. Итак, **модель** **угроз** – **это** документ, тем или иным способом описывающий возможные **угрозы** безопасности персональных данных.
* **Модель** **нарушителя** (в информатике) — абстрактное (формализованное или неформализованное) описание **нарушителя** правил разграничения доступа.
* **ЛВС** — локальная вычислительная сеть.
* **Firewall (межсетевой экран)** — программно-аппаратный комплекс, применяемый для разграничения доступа между сетями.
* **АРМ** – Автоматизированное рабочее место.
* **НГМД** — накопитель на гибких магнитных дисках.
* **СУБД** — система управления базами данных.
* **Notebook** — переносной персональный компьютер небольших размеров.
* **ПРД (Правила разграничения доступа)** — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.
* **Доступ к информации** — ознакомление с информацией, ее обработка, в частности: копирование, модификация или уничтожение информации.
* **Санкционированный доступ к информации** — доступ к информации, не нарушающий правила разграничения доступа.
* **НСД (Несанкционированный доступ к информации)** — доступ к информации, нарушающий правила разграничения доступа.
* **Доступность информации** — свойство системы, в которой циркулирует информация (средств и технологии ее обработки), характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.
* **Целостность информации** — свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).
* **Конфиденциальность информации** — субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

1. **Описание объекта защиты**

Основными объектами защиты системы информационной безопасности в компании ООО «Солнышко» являются:

* Информационные ресурсы, содержащие коммерческую тайну организации, личные данные сотрудников, базу данных компании, информацию, которая необходима для предоставления ее клиентам
* Информационные ресурсы, содержащие личные данные физических и юридических лиц
* Сотрудники компании, которые в своей работе взаимодействуют с данными информационной среды компании
* Информационная инфраструктура, которая содержит все данные о компании

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

Целью деятельности по обеспечению ИБ компании является снижение угроз ИБ до приемлемого уровня.

Задачами системы обеспечения информационной безопасности являются:

• Снижение операционных рисков, связанных с использованием информационных технологий;

• Оптимизация затрат на обеспечение информационной безопасности;

• выявление новых угроз;

• Контроль информационной безопасности на всех этапах цикла автоматизированных систем;

• Минимизация потерь компании при возникновении угроз информационной безопасности;

• Обеспечение безопасности его информационных активов в условиях неблагоприятных событий (экономические и политические кризисы, природные и техногенные катастрофы, террористические угрозы и пр.).

Безопасность информационных активов оценивается по:

• доступности

• целостности

• конфиденциальности

1. **Угрозы информационной безопасности**

* Угрозы конфиденциальности. Подобные угрозы могут возникать вследствие «человеческого фактора», сбоев работе программных и аппаратных средств. К информации ограниченного доступа относится
* Угрозы нарушения целостности — это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами — от умышленных действий персонала до выхода из строя оборудования.
* Угроза доступности. Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

1. **Модель нарушителя ИБ**

Внутренние нарушители:

* Пользователи информационной системы компании
* Сотрудники, у которых нет доступа к информационным ресурсам
* Сотрудники, имеющие доступ к информационным ресурсам
* Руководящие должности компании

Внешние нарушители:

* Бывшие сотрудники банка
* Представители компании, взаимодействующие с информационной структурой
* Клиенты
* Конкурирующие организации

Основные положения по обеспечению ИБ в Банке включают порядок управления рисками ИБ, инцидентами ИБ, защиту от утечек по техническим каналам, проверки по ИБ.

7.**Основные положения по обеспечению ИБ**

В соответствии с предписаниями федеральных законов Российской Федерации **целями защиты в информационной сфере**:

* предотвращение угроз безопасности конфиденциальной информации компании;
* предотвращение утечки, разглашения, утечки по техническим каналам, утраты (потери), хищения;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;
  1. **Организационная основа деятельности по обеспечению ИБ**

Ответственный подразделением – оперативная деятельность и планирование деятельности по обеспечению ИБ компании

В целях выполнения задач по обеспечению ИБ компании, в ней должно быть разделение на:

* Руководство – 5
* Бухгалтерия – 5
* IT-отдел – 5
* Менеджеры по работе с клиентами – 30
* Отдел безопасности – 5
* Куратор
  1. **Ответственность за соблюдение положений Политики**

За общее руководство по ИБ в компании ООО «Солнышко» отвечает куратор. Ответственность за поддержание политики ИБ лежит на руководстве Ответственного подразделения.

* 1. **Контроль за соблюдением положений ИБ**

Общий контроль состояния ИБ лежит на кураторе. Текущий контроль за соблюдением политики ИБ лежит на Ответственном подразделении. Контроль осуществляется путем проведения мониторинга.

* 1. **Заключительные положения**

В случае изменения законов или правовых документов, изменения в политике происходят только в тех аспектах, которые не противоречат новому закону. Ответственным за изменения является Ответственное подразделение.