«УТВЕРЖДАЮ»
Генеральный директор
ОАО «ФИРМА»
_____**Ф.И.О.**
«____» _____ 201_ год

КОНЦЕПЦИЯ
безопасности информации
ОАО «ФИРМА»

Город
201_ г.

Концепция безопасности информации ОАО «ФИРМА» (далее – Общество) основана на действующем законодательстве Российской Федерации и иных нормативно-правовых актах (Приложение №1), нормативно-методических материалах и организационно-распорядительных документах Общества.

Настоящая Концепция раскрывает основные понятия, связанные с безопасностью информации, обосновывает необходимость принятия мер по защите информации, определяет состав этих мер и этапы их реализации.

Основные положения данной Концепции не концентрируют внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

Концепция подлежит обязательному пересмотру, не реже одного раза в год. В течение этого периода в нее могут вноситься отдельные изменения и дополнения.

1. Термины и определения[1].
   - 1.1. Информация: сведения (сообщения, данные) независимо от формы их представления [2].
   - 1.2. Носитель информации: материальный объект, в том числе физическое поле, в котором информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин [9].
   - 1.3. Документ (документированная информация): зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию, или в установленных законодательством Российской Федерации случаях ее материальный носитель [2].
   - 1.4. Данные: факты, понятия или команды, представленные в формализованном виде и позволяющие осуществлять их передачу или обработку как вручную, так и с помощью средств автоматизации [9].
   - 1.5. Информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов [2].
   - 1.6. Пользователь информации: субъект, пользующийся информацией, полученной от ее обладателя или посредника, в соответствии с установленными правами и правилами доступа к информации либо с их нарушением [9];
   - 1.7. Обладатель информации: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [2].
   - 1.8. Доступ к информации: возможность получения информации и ее использования [2].
   - 1.9. Безопасность информации: состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность [9].
     - 1.9.1. Конфиденциальность информации: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [2].
     - 1.9.2. Доступность информации: состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно [9].
     - 1.9.3. Целостность: состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [9].
   - 1.10. Объект защиты информации: информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации [9].
   - 1.11. Политика безопасности (информации в организации): совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности [9].
   - 1.12. Конфиденциальность информации: обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя[3].
   - 1.13. Информация, составляющая коммерческую тайну (секрет производства): сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании, и в отношении которых обладателем таких сведений введен режим коммерческой тайны [3].
   - 1.14. Персональные данные: любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация [4].
   - 1.15. Руководители структурных подразделений: директора, начальники служб, отделов, их заместители,

[1] В данном разделе приведены термины, использованные в документе без описания их определений.

возглавляющие подразделения, напрямую подчиненные Генеральному директору Общества.

2. Общие положения.

2.1. Информация.

В общем понимании информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах, т.е. о ком-либо или о чем-либо. Информация не обладает признаками материального объекта до тех пор, пока не будет зафиксирована на материальном носителе (далее – носитель информации, носитель). Информация может быть зафиксирована на носителе, например, в текстовой форме, графической, звуковой, числовой, символьной, цифровой и других формах.

2.2. Информационные ресурсы.

Информационные ресурсы (далее - ИР) – это вся накопленная информация, зафиксированная на материальных носителях. ИР следует подразделять в первую очередь по признакам их принадлежности определенным субъектам, например, ИР Российской Федерации, ИР правительства РФ, ИР ОАО «ФИРМА» и т.п.

2.3. Информационная система.

Информационная система (далее – ИС) представляет собой совокупность информационных ресурсов и информационных технологий, в том числе, но не обязательно, с использованием средств вычислительной техники, телекоммуникаций и связи, поддерживающих информационные процессы.

ИС следует так же, как и ИР, подразделять по признакам их принадлежности определенному субъекту.

2.4. Информационные отношения, как предмет правового регулирования.

В ходе информационных процессов по сбору, обработке, накоплению, хранению, поиску, передаче, распространению и потреблению информации, между различными субъектами возникают общественные отношения, объектом которых является информация.

Законодательство РФ рассматривает информацию, как объект правовых отношений. В частности статья 5 [2] определяет: «Информация может являться объектом публичных, гражданских и иных правовых отношений». Таким образом, отношения, возникающие между различными субъектами, объектом которых является информация, подлежат регулированию государством (РФ) с помощью юридических норм.

2.5. Субъекты информационных отношений.

В процессе своей деятельности Общество выступает в роли одного из субъектов таких отношений. Другими субъектами информационных отношений могут выступать различные государственные органы, органы охраны правопорядка, общественные, политические, профессиональные объединения, юридические и физические лица.

По отношению к определенной информации различные субъекты могут выступать в качестве (роли):

- пользователей (потребителей) информации;
- обладателей информации.

При этом один и тот же субъект может выступать сразу в нескольких качествах (ролях) по отношению к определенной информации.

2.6. Безопасность информации.

Для успешного осуществления своей деятельности и защиты своих прав субъекты могут быть заинтересованы в обеспечении:

- своевременного доступа (за приемлемое для них время) к необходимой им информации;
- конфиденциальности определенной части информации;
- целостности (полноты, точности, достоверности) информации.

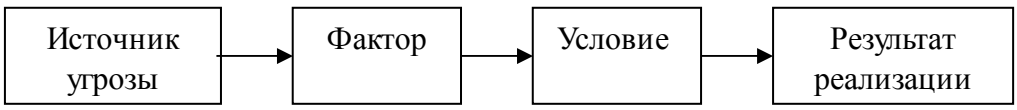
Будучи заинтересованным в обеспечении хотя бы одного из вышеназванных требований, субъект становится уязвимым, то есть потенциально подверженным нанесению ему ущерба (прямого или косвенного, материального или морального) посредством воздействия на важную для него информацию, ее носители и процессы обработки, либо посредством неправомерного использования такой информации.

2.7. Угрозы безопасности информации.

Угроза безопасности информации (далее – угроза): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [9]. Иными словами, угроза – это опасность нарушения конфиденциальности, доступности или целостности защищаемой информации. Угрозы можно классифицировать следующим образом:

- конфиденциальности информации – разглашение (раскрытие) конфиденциальной информации;
- доступности информации – уничтожение, блокирование информации или ее носителя;
- целостности информации – модификация (искажение) информации.

Схема реализации угроз может быть представлена в следующем виде:



В данной схеме:

- источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации [9];
- фактор – явление, действие или процесс, результатом которого может быть нарушение безопасности информации. Перечень факторов, которые могут воздействовать на защищаемую информацию, и их классификация приведены в [10].

Условием реализации угрозы является наличие или отсутствие реальных уязвимостей (недостатков, брешей и т.п.) в ИС и ее компонентах.

Результат реализации угрозы может быть положительным или отрицательным. При положительном результате реализации угрозы безопасность информации будет нарушена, а обладателю информации может быть нанесен ущерб.

2.8. Защита информации.

Защита информации – это деятельность субъекта, являющегося обладателем информации, обусловленная требованиями закона или договора направленная на исключение или минимизацию возможного ущерба от нарушений безопасности информации, путем воздействия на источники угроз и (или) ликвидации благоприятных условий для реализации этих угроз.

Состояние защищенности информации в ИС, т.е. ее безопасность, определяется состоянием защищенности всех компонентов ИС, задействованных в обработке, передаче, представлении и хранении данной информации. Таким образом, защита информации в ИС предполагает защиту, как отдельных компонентов ИС, так и самой системы в целом.

3. Безопасность информации Общества.

Принимая во внимание состояние и перспективы развития ИС Общества, требования Федеральных законов, увеличение объёмов обрабатываемой и хранимой (как с применением компьютерных систем, так и без их применения) информации, проводимые в Обществе мероприятия по защите информации должны иметь системный характер, опираться на соответствующие локальные нормативные акты, положения, инструкции. Такие нормативные акты должны регулировать не только вопросы защиты коммерческой тайны, но также:

- общей политики (принципов) информационной безопасности;
- прав и обязанностей пользователей информации;
- использования работниками ресурсов публичных информационных сетей, программного обеспечения, съёмных носителей информации.

В Обществе должна быть внедрена система обучения и информирования руководителей, работников по вопросам обеспечения информационной безопасности, а также система проверки состояния безопасности (аудита безопасности) и реагирования на нарушения, связанные с безопасностью информации.

Эти мероприятия позволят минимизировать риски нарушения конфиденциальности информации, иных угроз безопасности (см. п.2.7).

4. Основополагающие принципы обеспечения безопасности информации Общества.

Политика безопасности, нормативные акты по вопросам информационной безопасности и их применение должны основываться на следующих принципах:

4.1. Законность.

Применяемые требования, правила, процедуры безопасности информации должны соответствовать действующему законодательству РФ, документированы, утверждены и доведены до всех работников Общества.

4.2. Обязательность исполнения.

Устанавливаемые требования политики безопасности информации обязательны для исполнения всеми руководителями и работниками Общества.

4.3. Разумная достаточность.

Затраты на внедрение и осуществление мер защиты информации не должны превышать потенциальных потерь в случае, реализации соответствующих рисков, которые должны быть адекватно оценены. Имеет смысл рассматривать некоторый приемлемый уровень безопасности информации, при котором затраты, риски и размер возможного ущерба были бы разумно уравновешены.

4.4. Комплексность.

Обеспечение безопасности информации путем комплексного применения административных, организационных и технических мер защиты.

4.5. Непрерывность защиты.

Защита информации должна рассматриваться не как разовое мероприятие или простая совокупность принятых мер защиты, а как непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС.

4.6. Своевременность.

Разработка и совершенствование мер защиты информации должны вестись параллельно с разработкой и развитием ИС Общества.

4.7. Персональная ответственность.

Возложение ответственности за соблюдение требований политики безопасности информации на каждого работника Общества в пределах его полномочий.

4.8. Минимизация прав доступа к информации полномочий в ИС.

Доступ к информации должен предоставляться только тем лицам, которым эта информация необходима для выполнения возложенных на них обязанностей и только в том объеме (к той ее части), который необходим для выполнения определенных функций. Это справедливо и для предоставления полномочий в ИС Общества.

4.9. Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе пользователей, а также не должны требовать от них выполнения рутинных и малопонятных операций.

4.10. Обязательность контроля.

Предполагает обязательность и своевременность выявления и реагирования на нарушения безопасности информации.

5. Практические мероприятия по защите информации Общества.

Реализацию практических мероприятий целесообразно разбить на три этапа. Целью первого этапа должно стать достижение базового уровня безопасности информации, определяемого набором минимальных (базовых) требований безопасности. На втором этапе планируется внедрение системы анализа и оценки рисков, связанных с нарушениями безопасности информации и на основании результатов оценки рисков, выработка решения о принятии дополнительных мер защиты информации. На третьем этапе планируется внедрение системы менеджмента информационной безопасности, соответствующей требованиям национального стандарта ГОСТ Р ИСО/МЭК 27001-2006 [11] (аналог международного стандарта ISO/IEC 27001:2005).

В данной Концепции рассматривается первый (начальный) этап реализации практических мер по защите информации Общества. Этот этап рассчитан на один год. По окончании первого этапа Концепция будет пересмотрена, будут подведены итоги и определены цели и задачи, практические меры второго этапа и сроки их реализации.

5.1. Минимальные (базовые) требования безопасности.

Для достижения базового уровня безопасности информации в Обществе должно быть выполнено следующее:

- Разработана, документирована, доведена до всех работников и реализована политика безопасности информации;
- Организовано информирование работников по вопросам безопасности и защиты информации, и оперативное оповещение обо всех изменениях в политике безопасности информации, принимаемых мерах по ее защите, о нарушениях и инцидентах, связанных с безопасностью информации;
- Организован аудит безопасности информации;
- Организована система реагирования на нарушения требований, определяемых политикой безопасности информации;

Политика безопасности информации Общества должна регламентировать следующие вопросы:

- идентификации и аутентификации;
- предоставления и контроля доступа;
- антивирусной защиты;
- обеспечения конфиденциальности сведений, содержащих коммерческую тайну и персональных данных работников;
- использования программного обеспечения в Обществе;
- использования аппаратного обеспечения;
- бесперебойной работы ИС Общества;
- оборудования и защиты серверных помещений;
- использования доступа к ресурсам Интернет и средств электронной почты;
- персональной ответственности за соблюдение правил, определенных политикой безопасности Общества.

Система информирования и оповещения должна обеспечивать:

- быстрый и удобный доступ к документам по безопасности информации;
- своевременное оповещение работников Общества и третьих лиц обо всех изменениях в документах, определяющих политику безопасности информации, принимаемых мерах по защите информации, о нарушениях и инцидентах, связанных с безопасностью информации;
- проведение вводных и последующих инструктажей работников по общим правилам работы в ИС Общества, включающим в себя и правила обеспечения безопасности информации.

Система аудита безопасности информации должна обеспечивать:

- непрерывный сбор, документирование и хранение информации обо всех событиях, связанных с нарушениями безопасности информации;
- оперативное оповещение должностных лиц, отвечающих за поддержание безопасности информации;
- периодический анализ всех событий безопасности;
- создание отчетов и накопление аналитических материалов.

Система реагирования на нарушения требований действующей политики безопасности информации должна обеспечивать:

- немедленное принятие мер по фактам нарушений;
- расследование причин возникновения нарушений и определение круга лиц причастных к совершению данных нарушений;
- проведение разъяснительной, профилактической работы, оказание помощи работникам Общества по вопросам безопасности и защиты информации;
- накопление статистики.

5.2. Реализация практических мероприятий первого этапа.

Руководство реализацией практических мероприятий возлагается на Директора по режиму и экономической безопасности Общества.

5.2.1. Разработка, документирование и внедрение организационно - распорядительных документов, определяющих политику безопасности информации Общества.

В состав документов, определяющих политику безопасности информации Общества должны входить:

- политики – определяющие общие правила обеспечения безопасности информации и ответственность за нарушение этих правил;
- положения – устанавливающие права и обязанности, формы, порядок деятельности и ответственность должностных лиц;
- процедуры – устанавливающие последовательность действий для реализации конкретных задач;
- инструкции – определяющие правила выполнения операций, процессов, деятельности или правила пользования.

Все организационно – распорядительные документы, определяющие политику безопасности информации Общества, утверждаются и вводятся в действие приказом Генерального директора Общества. Этим приказом определяются перечень практических мероприятий по реализации требований вводимых в действие документов, сроки и ответственные за их выполнение.

Разработка политик и положений возлагается на Дирекцию по режиму и экономической безопасности (далее – ДРиЭБ) Общества. Необходимость разработки других документов (процедур и инструкций), сроки их разработки и ответственных за их разработку из числа руководителей структурных подразделений определяет Директор по режиму и экономической безопасности Общества, после утверждения каждой политики или положения Управляющим директором Общества.

Перечень политик и положений, разрабатываемых ДРиЭБ, приведен в Приложении №2.

5.2.2. Организация информирования и оповещения.

Оповещение работников Общества о выходе тех или иных документов по вопросам обеспечения безопасности информации следует организовать как установленным в Обществе порядком, так и с использованием средств электронной почты, а сами документы размещать на общедоступном внутреннем информационном ресурсе ИС Общества, для быстрого и удобного ознакомления с ними.

5.2.3. Организация аудита безопасности информации.

С целью определения эффективности проводимой политики безопасности информации и оперативного реагирования на нарушения, связанные с безопасностью информации, в Обществе должна быть организована система аудита безопасности информации. Для этих целей Дирекцией по информационным технологиям (далее – ДИТ) должен быть организован непрерывный сбор, накопление и хранение информации обо всех событиях безопасности, имевших место в операционных системах, системах управления базами данных, прикладных программах и приложениях.

Анализ этих событий, разработка практических мероприятий по защите информации на основе результатов анализа, накопление аналитической информации проводятся ДРиЭБ. Результаты анализа в виде ежемесячных и годовых отчетов должны предоставляться руководству Общества для ознакомления и оценки эффективности принимаемых мер по защите информации.

5.2.4. Организация реагирования на нарушения безопасности информации.

Любое нарушение требований действующего законодательства РФ, установленных в Обществе правил безопасности информации, совершенное работниками Общества или представителями третьих лиц должно быть расследовано работниками ДРиЭБ, при необходимости, с привлечением специалистов других подразделений Общества. В результате расследования должны быть выявлены причины и определен круг лиц, причастных к совершению данного нарушения.

Параллельно с проведением расследования ДРиЭБ, совместно с ДИТ должны быть разработаны и приняты меры, направленные на быструю ликвидацию или уменьшение негативных последствий и дополнительные меры по защите информации.

Доступ к результатам расследований должен быть ограничен кругом лиц, участвующих в проведении

расследований и лиц, принимающих решение по фактам нарушений. Информация, в части касающейся, может быть передана третьей стороне, в случаях проведения расследования в отношении ее работников, а также правоохранительным органам в случаях нарушений действующего законодательства РФ.

К виновным должны применяться меры воздействия, соответствующие совершенному нарушению. При этом должна учитываться серьезность нарушения, наличие в действиях работника или отсутствие злого умысла и другие факторы.

В целях профилактики нарушений работниками ДРиЭБ и ДИТ должна проводиться разъяснительная работа среди работников Общества по вопросам соблюдения требований действующей политики безопасности информации.

Приложение:

1. Перечень Документов, использованных при разработке Концепции на 1 л. в 1 экз.
2. Перечень политик и положений, разрабатываемых ДРиЭБ на 1 л. в 1 экз.
3. Лист согласования на 1 л. в 1 экз.

Директор по режиму и экономической безопасности ОАО «ФИРМА» **Ф.И.О.**

Приложение №1
к Концепции безопасности информации
ОАО «ФИРМА»
(на одном листе)

Перечень Документов, использованных при разработке Концепции:

1. Гражданский кодекс РФ (часть четвертая) от 18.12.2006 г. № 230-ФЗ.
2. Федеральный закон РФ № 149-ФЗ от 27.07.2006 г. «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон РФ № 98-ФЗ от 29.07.2004 г. «О коммерческой тайне».
4. Федеральный закон РФ № 152-ФЗ от 27.07.2006 г. «О персональных данных».
5. Федеральный закон РФ № 208-ФЗ от 26.12.1995 г. «Об акционерных обществах».
6. Постановление правительства РФ № 781 от 17.11.2007 г. «Об утверждении положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных».
7. Постановление правительства РСФСР № 35 от 05.12.1991 г. «О перечне сведений, которые не могут составлять коммерческую тайну".
8. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».
9. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения».
10. ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».
11. ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности».
12. Указ Президента РФ №188 от 06.03.1997 года «Об утверждении перечня сведений конфиденциального характера».

Приложение №2
к Концепции безопасности информации
ОАО «ФИРМА»
(на одном листе)

Перечень политик и положений, разрабатываемых ДРиЭБ[2]:

- «Положение о конфиденциальной информации и мерах по ее защите». Данный документ должен ввести категорирование информации по степени ее конфиденциальности, определить меры по защите конфиденциальной информации, правила работы с ней, обязанности работников и должностных лиц по защите конфиденциальности этой информации и ответственность за нарушения.
- «Политика использования информационных ресурсов Общества». Данный документ должен определить структуру информационных ресурсов, общие правила хранения и обработки информации, определить подразделения, отвечающие за использование тех или иных информационных ресурсов.
- «Политика предоставления и контроля доступа». Данная политика должна определить правила предоставления и контроля доступа к оборудованию ИС, в помещения, где оно установлено, доступа к информационным ресурсам, системам и приложениям, правила идентификации и аутентификации.
- «Политика предоставления и контроля доступа третьим лицам». Данная политика должна определить правила предоставления и контроля доступа к оборудованию ИС, в помещения, где оно установлено, доступа к информационным ресурсам, системам и приложениям третьим лицам при проведении работ по обслуживанию, ремонту, монтажу и демонтажу оборудования ИС, предоставлении услуг и организации информационного обмена;
- «Политика использования программного обеспечения». Данный документ должен определить правила закупки, учета, хранения, инсталляции (деинсталляции) программного обеспечения, учета и хранения регистрационной информации.
- «Политика использования беспроводных сетей». Данный документ должен определить правила использования беспроводных компьютерных сетей в Обществе.
- «Политика антивирусной защиты». Данный документ должен определить общие правила организации антивирусной защиты в Обществе.
- «Политика резервного копирования информации». Данная политика должна определить общие правила организации резервного копирования в Обществе, а именно, объем и периодичность резервного копирования, правила учета, хранения, выдачи резервных копий, правила уничтожения носителей с резервными копиями.
- «Политика использования портативных технических устройств, способных накапливать и хранить информацию в электронном виде». Данная политика должна определить общие правила использования в Обществе различных технических устройств: flash-накопителей, фотоаппаратов, сотовых телефонов и т.п.
- «Политика использования доступа к ресурсам Интернет и средств электронной почты». Данная политика должна определить общие правила использования доступа к ресурсам Интернет, средств электронной почты, а также правила безопасной работы при использовании этих сервисов.

Специалист по информационной безопасности
службы экономической безопасности **Ф.И.О.**

[2] Перечень документов может быть изменен или дополнен.

Приложение №3
к Концепции безопасности информации
ОАО «ФИРМА»
(на одном листе)

Лист согласования
Концепции безопасности информации
ОАО «ФИРМА»

№№ п/п	Должность	Подпись	Фамилия, инициалы	Дата
1	Директор по эксплуатации		Ф.И.О.	
1	Директор по экономике и финансам		Ф.И.О.	
2	Директор по персоналу и общим вопросам		Ф.И.О.	
3	Директор по информационным технологиям		Ф.И.О.	
4	Директор по правовым и корпоративным вопросам		Ф.И.О.	
5	Директор по режиму и экономической безопасности		Ф.И.О.	
6	Начальник правового управления		Ф.И.О.	
7	Начальник протокольного отдела		Ф.И.О.	