УДК 004.056.5

С.В. Корякин,srgkoryakin1@gmail.com
Институт информационных технологий КГТУ им. И.Раззакова
Институт машиноведения автоматики и геомеханики НАН КР
А.Т. Рысалиева, ainazikrysalievaaa@gmail.com
И.В. Якимчук, iliyakg@gmail.com
Т.Н. Марченко, Homenko_tanya@mail.ru
Институт информационных технологий КГТУ им. И.Раззакова

АНАЛИТИЧЕСКИЙ ОБЗОР ПОДХОДОВ К РАЗРАБОТКЕ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

В настоящее время, когда угрозы информационной безопасности достигли невиданных ранее масштабов, вопросы информационной безопасности и устойчивого развития автоматизированных информационных систем (АИС) приобретают особую сторону. Неуклонно возрастающее давление на АИС злоумышленниками и киберпреступниками, одновременно усиливаемое деятельностью сотрудников обслуживающих и эксплуатирующих эти системы, активизирует необходимость применения комплексного подхода в обеспечении защиты информации в АИС и тщательного анализа состояния защищенности всех компонентов и подсистем, входящих в состав АИС. В этом свете наблюдение за состоянием защищенности АИС является центральным аспектом для оценки и прогноза изменений, вызванных в результате воздействия от деятельности внешних и внутренних угроз безопасности информации. Это не только позволяет отслеживать состояние защищенности АИС от угроз ИБ, но и выявлять тенденции изменений уровня их модификации и развития, оценивать возможные риски и уровень ущерба, нанесённого инцидентами ИБ. Сложность и значимость этой проблемы требуют применения новейших технологий и подходов. Одним из ключевых шагов, необходимых для решения проблемы, является качественная разработка политики информационной безопасности в АИС. В данной работе подробно рассматриваются этапы разработки и различные подходы и методы разработки политики информационной безопасности, включая нормативный, рисковый, проактивный, реактивные подходы. Проведен сравнительный анализ этих подходов с точки зрения их преимуществ и недостатков. Представлены рекомендации по использованию комбинированного подхода для создания эффективной системы защиты информации, обеспечивающей всестороннюю безопасность информации, передаваемой, хранимой и обрабатываемой в АИС.

Ключевые слова: информационная безопасность (ИБ), политика ИБ, технологии защиты информации, риски, аудит ИБ, ISO/IEC 27001, DLP, IDS, SIEM, антивирусы, автоматизированные информационные системы (АИС).

Современное состояние требований и подходов к разработке политики ИБ

В условиях цифровой трансформации и глобализации бизнеса информационная безопасность становится приоритетной задачей для любой организации. Постоянное развитие информационных технологий и увеличение объемов обрабатываемых данных требуют создания эффективной системы защиты информации. Политика информационной безопасности представляет собой стратегический документ, который определяет правила и процедуры для защиты информации от различных угроз, включая кибератаки, утечки данных, внутренние злоупотребления и природные катастрофы.

В настоящее время современные организации сталкиваются с множеством угроз информационной безопасности, включая кибератаки, вирусы, внутренние злоупотребления и случайные утечки данных. Недостаточная защита информации может привести к серьезным последствиям, таким как финансовые потери, ущерб репутации и юридические санкции. Принято считать, что решение одной из главных проблем заключается в необходимости разработки и внедрения эффективной политики информационной безопасности, которая бы обеспечивала защиту данных на всех уровнях жизненного цикла АИС.

Как правило, политика информационной безопасности – это высокоуровневый документ, который включает в себя принципы и правила, определяющие и ограничивающие определенные виды деятельности объектов и участников системы информационной безопасности, направленные на защиту информационных ресурсов организации [2].

На сегодняшний день большинство крупных предприятий понимает всю серьёзность разработки этого сегмента. Очевидно, что одной только организационной работы с сотрудниками и обычной антивирусной защиты недостаточно, поскольку современный мир развивается быстрыми темпами, компании-конкуренты, мошенники и другие лица нередко ищут различные способы для того, чтобы проникнуть в базу данных процветающих компаний. Защита всей информации от кражи (или ненамеренной потери) приводит к необходимости разработки политики безопасности, включающей системные меры противодействия угрозам[3].

Как правило, разработка политики информационной безопасности основывается на нескольких ключевых принципах и стандартах. Важнейшими международными стандартами являются ISO/IEC 27001, который предоставляет требования к системе управления информационной безопасностью, и ISO/IEC 17799, который содержит кодекс практики для управления информационной безопасностью. ГОСТ Р ИСО/МЭК 15408 (Критерии оценки безопасности информационных технологий) также играет важную роль в формировании требований к безопасности ИТ-систем и АИС [4]. На рисунке 1 изображены основные цели политики ИБ.

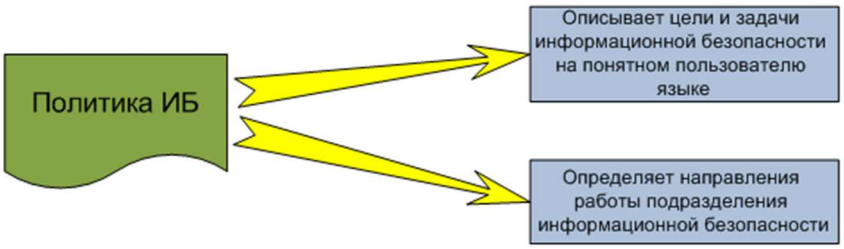

Рисунок 1 – Цели политики ИБ

На сегодняшний день руководителями организаций и бизнеса все чаще и чаще ставится вопрос о том, какие риски несет отсутствие политики информационной безопасности.

Считается, что основными рисками отсутствия политики информационной безопасности являются: потеря компанией влияния на рынке, потеря отдельных секторов рынка, ухудшение репутации организации, риск потери клиентов, риски снижения прибыли, потеря собственных разработок в случае кражи информации, отзыв лицензии и другие.

В финансовом плане все эти риски оцениваются достаточно высоко. Поэтому руководителям бизнеса нужно приложить все силы к разработке системы, направленной на защиту конфиденциальной информации и на снижение рисков, приводящих к значительному ущербу активов организации[3].

Разработку политики ИБ условно можно разделить на следующие основные этапы:

роведение аудита информационной безопасности:

- *Оценка текущего состояния ИБ в организации.*
- *Выявление уязвимостей и потенциальных угроз.*
- *Определение критически важных информационных ресурсов.*

нализ рисков:

- *Идентификация и оценка рисков для информационных систем.*
- *Разработка стратегий управления рисками.*
- *Приоритезация рисков и планирование мер по их снижению.*

азработка требований и решений по защите информации:

- *Определение политик и процедур для защиты данных.*
- *Разработка технических и организационных мер.*
- *Определение ответственности за выполнение мер ИБ.*

оздание нормативных документов:

- *Разработка и утверждение политики информационной безопасности.*
- *Подготовка инструкций и регламентов.*
- *Обучение сотрудников и повышение их осведомленности о ИБ.*[4]

На рисунке 2 приведена функциональная блок-схема «Основные этапы разработки политики ИБ»:

Рисунок 2 – Основные этапы разработки политики ИБ

Таким образом, можно говорить о том, что современная система информационной безопасности представляет собой синтез организационных и программно-технических мер, реализованных на основе единого подхода. При этом организационные меры не менее важны, чем технические – без внедрения безопасных приемов работы и осознания необходимости принимаемых мер немыслимо создать действительно защищенную инфраструктуру безопасности.

Для обеспечения эффективной защиты информации организациям необходимо использовать как организационные, так и технические меры.

Считается, что организационные меры включают в себя разработку внутренних регламентов, инструкций и процедур по работе с конфиденциальной информацией.

Технические меры включают использование различных средств защиты, таких как системы предотвращения утечек данных (DLP), антивирусные программы, системы обнаружения вторжений (IDS), системы управления событиями и инцидентами безопасности (SIEM) и другие.

В качестве основных организационных мер, входящих в состав работ по разработке политики ИБ, выделяют следующие:

- **Разработка внутренней документации**:
  - Политики ИБ, инструкции и регламенты.
  - Процедуры управления доступом и идентификации.
  - Процедуры обработки инцидентов информационной безопасности.
- **Обучение и повышение осведомленности сотрудников**:
  - Регулярные тренинги и курсы по ИБ.
  - Проведение учебных атак и симуляций для проверки готовности.
  - Разработка программы мотивации за соблюдение политики ИБ.

Кроме того, как правило, принято использовать ряд вспомогательных мер, входящих в состав работ по разработке политики ИБ, которые включают в себя:

разработку мероприятий, регламентирующих допуск посторонних лиц на объект, допуск посторонних лиц к документации, разработку и планирование мероприятий, связанных с обучением сотрудников, контролем знаний, аттестацией в сфере работы с важной информацией, определение ответственности за нарушение правил взаимодействия с конфиденциальной информацией и определение порядка привлечения к ответственности персонала, разработку системы авторизации и другие.

К техническим мерам, как правило, относят:

- **Системы предотвращения утечек данных (DLP)**:
  - Мониторинг и контроль передачи данных.
  - Защита конфиденциальной информации от несанкционированного доступа.

- Обнаружение и блокирование подозрительных действий.

- **Системы управления событиями и инцидентами безопасности (SIEM)**:
  - Сбор, анализ и корреляция данных о событиях безопасности.
  - Обнаружение аномалий и подозрительной активности.
  - Реагирование на инциденты и их расследование.
- **Антивирусные программы и системы обнаружения вторжений (IDS)**:
  - Защита от вредоносного ПО и вирусов.
  - Обнаружение и предотвращение несанкционированного доступа.
  - Анализ трафика и обнаружение атак [3].

Структура политики информационной безопасности

Принято считать, что процесс подготовки и утверждения политики информационной безопасности может занять до шести месяцев, начиная с аудита и завершая сертификацией системы. Документация, разработанная и утвержденная в ходе этого процесса, должна включать следующие разделы, графически изображенные на рисунке 3.

Рисунок 3 – Перечень документации, входящей в состав политики ИБ

Перечень объектов информационной безопасности: Указание всех объектов, для которых устанавливаются меры защиты, с ранжированием по значимости и степени необходимой защиты.

Описание функций подразделений: Описание функций каждого подразделения, ответственного за обработку и защиту данных, а также функций самой системы информационной безопасности.

Описание применяемых технологий: Детализация технологий, используемых для обеспечения сохранности информации.

Перечень угроз: Список существующих и потенциальных угроз информационной безопасности, оценка их серьезности и вероятности реализации.

Модель угроз: Моделирование вероятных способов проникновения через защитные контуры информационной безопасности.

Описание угроз: Характеристика внешних и внутренних субъектов, которые могут представлять потенциальную угрозу.

Принципы и стандарты защиты: Описание общих принципов и стандартов, основанных на ISO/IEC 27001-2005 и соответствующих российским ГОСТам.

Административные меры: Описание административных мер, документов и стандартов, применяемых для обеспечения информационной безопасности.

Инциденты ИБ: Определение понятия инцидента информационной безопасности и процедуры уведомления о его возникновении.

Организационные меры: Описание действий сотрудников по обеспечению информационной безопасности.

Системы доступа: Описание систем доступа к информационным ресурсам организации, ранжирование уровней доступа в зависимости от должности, соответствия требованиям безопасности и важности охраняемых данных.

Антивирусная защита: Описание политики защиты от вирусных атак, вредоносных программ и возможных действий хакеров.

Резервное копирование: Описание системы резервного копирования важных данных, периодичность и модели хранения (диски, удаленные серверы).

Аварийные и восстановительные работы: Описание порядка проведения аварийных и восстановительных работ при повреждении аппаратной части вследствие пожара, проблем с электросвязью или других причин, приводящих к потере данных.

Тестирование и сертификация: Описание процесса тестирования, согласования, аттестации и сертификации системы в соответствии с ISO/IEC 27001-2005 и российскими стандартами. Процесс сертификации необходим для обеспечения возможности работы с данными ограниченного доступа и получения лицензий.

Расследование инцидентов: Описание системы расследования инцидентов информационной безопасности, включая привлечение компетентных организаций или правоохранительных органов.

План мероприятий: План действий по поддержанию готовности системы к работе, ее обновлению при изменении правил сертификации или степени значимости угроз.

Большинство разделов должны быть общими и отсылать к конкретным стандартам и регламентам. Документ должен быть понятным для всех пользователей компании, а специализированные термины — только для узких специалистов.

Несмотря на объем и сложность темы, необходимо соблюдать следующие требования:

Лаконичность: Документ должен быть достаточно компактным (не более 150—200 страниц), чтобы его можно было прочитать и применять.

Простота изложения: Рекомендации должны быть изложены максимально простым и понятным языком, чтобы даже администратор мог легко их понять и выполнить.

Исходя из вышеперечисленного, следует, что все регламенты, содержащие процессы, уровни ответственности и графические схемы, должны быть вынесены в приложения. Для этого предлагается разработать трехуровневую систему документации, структура которой изображена на рисунке 4.

Проводя анализ способов подготовки документов подобного рода, можно выделить примеры противоположных друг другу подходов к подготовке пакетов документов, к примеру, состав документации, входящий в пакет документов при использовании так называемого максималистического подхода, включающего в себя всевозможные варианты регламентов и инструкций, состоит минимум из 45 страниц, насыщенных специальными терминами, сложными в понимании и осознании большинства сотрудников организации, в то время как аналогичный документ с использованием минималистического подхода занимает всего 11 страниц и изложен простым и понятным языком.

При этом считается, что при подготовке пакета документов подобного рода очень важно учитывать производственные, территориальные и кадровые факторы, которые определяют специфику мер защиты. Система и политика безопасности должны максимально учитывать особенности работы каждого юридического лица, включая графики, территории и ресурсы. Все это должно гарантировать высокую степень защиты при минимальных финансовых затратах. При этом после внедрения политики ИБ производительность труда не должна страдать от излишнего количества регламентов.

Рисунок 4 – Структура трехуровневой система документации

Кроме того, следует понимать, что сертификация, аттестация и внедрение новых программных продуктов требуют пересмотра бюджета, выделяемого на разработку политики ИБ и построения системы защиты информации в целом. Именно поэтому рекомендуется своевременно подготавливать сметный расчет и согласовывать бюджет на уровне высшего руководства. В крупных компаниях бюджетное планирование осуществляется на уровне квартала и года. По статистике, среднее время, необходимое на внедрение политики ИБ, как правило, может занять не менее двух кварталов[4].

Считается, что разработка политики ИБ с учетом современных процедур и программных продуктов, таких как DLP и SIEM-системы, требует не только финансовых, но и временных ресурсов. Поэтому своевременное планирование средств и согласование их привлечения зависит напрямую от подразделений, отвечающих за подготовку политики ИБ.

Исходя из вышеперечисленного, следует, что системная работа в области информационной безопасности требует внимания не только специализированных подразделений, но и кадровых, финансовых, бухгалтерских служб, а также руководства компании. Все сотрудники должны быть уведомлены о целях разработки этой системы и лично заинтересованы в успешной ее реализации. В этом помогут системы мотивации, связывающие ключевые показатели эффективности с соблюдением требований политики и успешным ее внедрением [5].

Основные подходы к разработке политики информационной безопасности

В настоящее время специалистами по ИБ рекомендуется множество подходов и требований к разработке политики ИБ. Они, как правило, включают в себя требования международных стандартов по информационной безопасности, таких как ISO 27001, PCIDSS, ГОСТы, стандарты ФСТЕК РФ, Закон о кибербезопасности КР, Цифровой кодекс КР и др. Поэтому, исходя из требований стандартов по ИБ, следует выделить следующие основные подходы, наиболее полноценно описывающие процесс разработки политики ИБ организаций

1. Подход на основе нормативных требований.
2. Подход на основе управления рисками.
3. Проактивный подход.
4. Реактивный подход.

1. Подход на основе нормативных требований

Принято считать, что подход на основе нормативных требований фокусируется на соблюдении различных законов, регуляторных актов, стандартов и отраслевых норм. Основная цель этого подхода заключается в том, чтобы обеспечить соответствие организации установленным нормативным требованиям для минимизации юридических рисков и предотвращения санкций [7]. На рисунке 5 в обобщенном виде представлена функциональная блок-схема такого подхода.

Рисунок 5– Функциональная блок-схема подхода к разработке политики ИБ на основе нормативных требований.

Считается, что к основным стандартам и нормативным документам, используемым в рассматриваемом подходе, относятся:

Международный стандарт по управлению информационной безопасностью.

Определяет требования к созданию, внедрению, эксплуатации, мониторингу, обзору, поддержанию и улучшению системы управления информационной безопасностью (СУИБ).

Рамочная структура для управления кибербезопасностью, разработанная NIST.

Содержит рекомендации по идентификации, защите, обнаружению, реагированию и восстановлению после кибератак.

Общий регламент по защите данных в ЕС.

Устанавливает требования по защите персональных данных и правам субъектов данных.

- **ГОСТ Р 57580**:

Российский стандарт по защите персональных данных.

Определяет требования к мерам защиты информации при обработке персональных данных в информационных системах.

Таким образом, исходя из вышеизложенного, следует, что использование подхода на основе нормативных требований помогает организациям создавать эффективные и надежные системы информационной безопасности, соответствующие требованиям законодательств и лучшим мировым практикам [8].

2. Подход на основе управления рисками

Считается, что подход на основе управления рисками ориентируется на идентификацию, оценку и управление рисками, связанными с информационной безопасностью. Основная цель этого подхода заключается в приоритизации ресурсов и мер безопасности для защиты наиболее критических активов и минимизации возможных последствий инцидентов.

Другими словами, подход на основе управления рисками при разработке политики ИБ можно объяснить как процесс, в котором компания старается заранее понять, какие из существующих угроз ИБ могут оказывать воздействие на работоспособность информационной системы в целом, и придумать, как противодействовать потенциальным

угрозам [9]. На рисунке 6 в обобщенном виде представлена функциональная блок-схема подхода к разработке политики ИБ на основе управления рисками.

Рисунок 6 – Функциональная блок-схема подхода к разработке политики ИБ на основе управления рисками

3. Проактивный подход

Принято считать, что проактивный подход к разработке политики ИБ включает в себя меры для предотвращения инцидентов ИБ заблаговременно до их возможного возникновения. Как правило, набор основных мероприятий может состоять из регулярных тестов на проникновение, анализа уязвимостей, мониторинга сетевой активности и многих других проактивных мер, направленных на обеспечение ИБ [10]. На рисунке 7 в обобщенном виде представлена функциональная блок-схема проактивного подхода к построению политики ИБ.

Рисунок 7– Функциональная блок-схема проактивного подхода к процессу построения политики ИБ

Таким образом, из рисунка 7 видно, что проактивный подход при разработке политики информационной безопасности позволяет организациям предвосхищать и предотвращать угрозы, минимизируя риск инцидентов и их последствия. Несмотря на сложности и затраты на реализацию, этот подход обеспечивает высокий уровень защиты и устойчивость к киберугрозам, что делает его крайне эффективным в современных условиях.

4. Реактивный подход

Как правило, принято считать, что реактивный подход к разработке политики ИБ фокусируется на быстром реагировании на инциденты ИБ и минимизации ущерба после их возникновения. Это включает в себя разработку и внедрение процедур инцидент-менеджмента, планов восстановления и других мер по устранению последствий инцидентов. Другими словами, отличие от проактивного подхода, который предполагает предотвращение угроз, реактивный подход направлен на быструю и эффективную реакцию на уже произошедшие инциденты. На рисунке 8 в обобщенном виде представлена функциональная блок-схема реактивного подхода к разработке политики ИБ.

Рисунок 8 – Функциональная блок-схема реактивного подхода к разработке политики ИБ

Как правило, реактивный подход при разработке политики информационной безопасности может быть полезен для быстрой реакции на уже произошедшие инциденты. Однако его недостатки, такие как высокий риск инцидентов ИБ, способных нанести ущерб и большие затраты на восстановление последствий, нанесенных этими инцидентами, делают его менее предпочтительным в долгосрочной перспективе по сравнению с проактивным подходом

Следует отметить, что, помимо подходов к построению политики ИБ в процессе реализации мероприятий, входящих в дорожную карту процесса построения политики ИБ, используются конкретные методы реализации описанных выше подходов. Считается, что методы являются более конкретными действиями и техниками, которые реализуют выбранные подходы к разработке политики ИБ.

Методы проактивного подхода. В случае, если организация выбирает проактивный подход к построению политики и системы информационной безопасности, она может использовать следующие методы:

егулярный анализ рисков для выявления потенциальных угроз.

ониторинг сети и систем для обнаружения аномалий.

роведение регулярных тренингов для сотрудников по вопросам безопасности[12].

Методы реактивного подхода. Если организация выбирает реактивный подход к информационной безопасности, она может использовать следующие методы:

истемы реагирования на инциденты для быстрого устранения последствий атак.

огирование и анализ событий для расследования инцидентов.

бучение сотрудников действиям в случае инцидентов безопасности.

Методы подхода на основе управления рисками. При использовании подхода на основе управления рисками к информационной безопасности могут применяться следующие методы:

егулярный анализ и оценка рисков для определения приоритетов защиты.

азработка и внедрение мер управления рисками.

остоянный мониторинг и пересмотр рисков в связи с изменениями в окружении и технологии.

Методы подхода на основе нормативных требований. Если организация выбирает подход на основе нормативных требований к информационной безопасности, могут использоваться следующие методы:

нализ нормативных требований и стандартов для выявления обязательных мер безопасности.

азработка политики ИБ в соответствии с требованиями нормативных актов.

егулярные аудиты и оценки соответствия для обеспечения соблюдения стандартов и нормативов [13].

Исходя из описанного выше, следует, что представленные подходы и методы имеют свои преимущества и недостатки, которые после реализации политики ИБ с использованием того или иного метода напрямую повлияют на уровень состояния защищенности информационной системы в целом. Именно поэтому перед утверждением подхода по реализации политики ИБ

специалистам следует проводить сравнительный анализ функциональных особенностей подходов к разработке политики ИБ.

В таблице 1 представлен сравнительный анализ функциональных особенностей, рассмотренных в работе подходов к разработке политики ИБ[14].

Таблица 1. Сравнительный анализ функциональных особенностей подходов к разработке политики ИБ

Критерий / Функциональная особенность	Подход на основе нормативных требований	Подход на основе управления рисками	Проактивный подход	Реактивный подход
Описание	Основывается на соблюдении нормативных актов и стандартов (например, ISO/IEC 27001, ГОСТ)	Определение и управление рисками для минимизации их воздействия на организацию	Предупреждение угроз до их реализации через постоянный мониторинг и улучшение мер безопасности	Реагирование на инциденты и угрозы по мере их возникновения
Преимущества	Соответствие нормативным требованиям и стандартам. Структурированный и четкий подход. Простота внедрения	Снижение вероятности и воздействия инцидентов. Оптимальное использование ресурсов. Фокус на критически важных активах	Предупреждение инцидентов. Повышенная устойчивость к угрозам. Постоянное улучшение безопасности	Быстрая реакция на реальные угрозы. Меньшие первоначальные затраты. Фокус на актуальных проблемах
Недостатки	Ограниченная гибкость. Возможное несвоевременное обновление мер безопасности. Высокие затраты на соответствие нормативным актам	Сложность реализации. Высокие требования к квалификации сотрудников. Возможность недооценки рисков	Высокие первоначальные затраты. Сложность реализации и поддержания. Необходимость постоянного мониторинга	Высокий риск серьезных инцидентов. Большие затраты на восстановление. Стресс и нагрузка на сотрудников
Цель	Обеспечение соответствия нормативным требованиям и стандартам	Идентификация, оценка и управление рисками для минимизации их воздействия	Предупреждение и минимизация угроз до их реализации	Быстрая и эффективная реакция на уже произошедшие инциденты
Требования к ресурсам	Средние: требуется знание нормативных актов и стандартов	Высокие: требуются специалисты по управлению рисками и ИБ	Высокие: необходимы средства мониторинга, обновления и квалифицированные специалисты	Низкие/Средние: фокус на реагировании, меньше затрат на профилактику

Примеры мер безопасности	Политики и процедуры, соответствующие стандартам (ISO/IEC 27001, ГОСТ)	Анализ рисков, разработка плана управления рисками, проведение аудиторов	Постоянный мониторинг систем, регулярные обновления, тренировки сотрудников	Системы мониторинга и оповещения, планы реагирования на инциденты, документация инцидентов
Обучение сотрудников	Регулярное обучение по соблюдению нормативных требований	Обучение по оценке и управлению рисками	Постоянное обучение и тренировки для повышения осведомленности о новых угрозах	Обучение правильным действиям в случае инцидентов
Гибкость	Низкая: жестко следует нормативным требованиям	Средняя: позволяет адаптировать меры в зависимости от рисков	Высокая: адаптируется к изменяющемуся ландшафту угроз	Низкая: реагирует на уже произошедшие инциденты
Долгосрочная эффективность	*Средняя*: обеспечивает базовую защиту, но может отставать от новых угроз	*Высокая*: постоянно адаптируется и улучшает меры безопасности	*Очень высокая*: предупреждает инциденты и минимизирует угрозы	*Низкая*: может справляться с угрозами по мере их появления, но не предотвращает их

Таким образом, результаты представленного в таблице 1 подробного сравнительного анализа рассматриваемых в работе подходов к разработке политики информационной безопасности смогут помочь специалистам определить наиболее подходящий подход в зависимости от конкретных потребностей и ресурсов организации.

Следует отметить, что комбинирование проективных и реактивных мер в подходе к разработке политики ИБ может обеспечить более надежную и эффективную защиту информационных ресурсов организации.

Подводя итог проведенного анализа (таблица 1), для построения политики ИБ рекомендуется использовать **комбинированный подход, сочетающий в себе методы управления рисками, и проактивный подход как наиболее эффективный и способный обеспечить по сравнению с другими подходами, более максимальную защиту от угроз ИБ.** На рисунке 9 в обобщенном виде представлена функциональная блок-схема комбинированного подхода к разработке политики ИБ.

Рассмотрим основные критерии подхода, характеризующие его как наиболее оптимальный для построения политики ИБ:

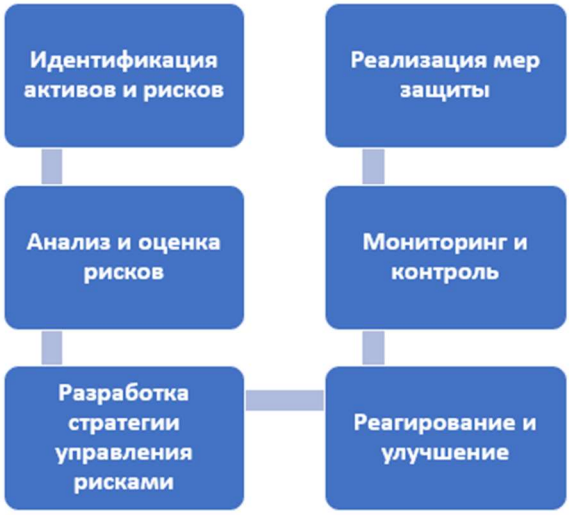

Рисунок 9 — Обобщенная функциональная блок-схема комбинированного подхода к разработке политики ИБ

Всесторонняя защита: Комбинация управления рисками и проактивного подхода обеспечивает всестороннюю защиту информации. Управление рисками позволяет сосредоточиться на защите наиболее критических активов и эффективно распределять ресурсы, тогда как проактивный подход предотвращает угрозы до их реализации.

Экономическая эффективность: Управление рисками помогает оптимизировать затраты на безопасность, направляя их на наиболее значимые области. Проактивные меры, несмотря на высокую стоимость, снижают потенциальный ущерб и расходы на восстановление после инцидентов.

Адаптивность и гибкость: Комбинированный подход обеспечивает гибкость и возможность адаптироваться к изменяющимся угрозам и условиям.

Постоянное улучшение: Проактивные меры способствуют постоянному улучшению мер безопасности, что в сочетании с управлением рисками повышает общую устойчивость системы ИБ.

Следует отметить, что выбор эффективного подхода для построения политики ИБ не дает стопроцентной гарантии защищенности информации, хранящейся в ИС от угроз ИБ, поскольку развитие науки и техники, сам научно-технический прогресс не стоят на месте. Каждый день в мире информационных технологий появляются новые схемотехнические, технологические инновационные решения и способы обработки и хранения информации при помощи технологий микропроцессорных систем. Появляются новые языки программирования, способы построения и проектирования микросхем и технологий использования полупроводниковых элементов, которые открывают новые возможности в использовании технических элементов, используемых для обработки и хранения информации, что приводит к повышению технических характеристик устройств обработки данных и, как следствие, повышение производительности ПО используемого для обработки и хранения информации. Все это позволяет злоумышленникам получать и использовать новые способы реализации угроз ИБ, что в свою очередь приводит к снижению состояния защищенности ИС от киберугроз.

Именно поэтому построения и утверждения политики ИБ с использованием одного из перечисленных выше подходов в обязательном порядке рекомендуется выполнять на периодической основе (как минимум 2 раза в год) следующие организационные мероприятия:

- На основании приказа об утверждении политики ИБ под подпись ознакомить с политикой ИБ всех работающих сотрудников организации или предприятия;
- При приеме новых сотрудников на работу в обязательном порядке ознакамливать под подпись с политикой ИБ всех новых сотрудников;

• На регулярной основе производить анализ текущих бизнес/технологических-процессов с целью выявления и минимизации рисков;

• При разработке новых бизнес-процессов проводить согласование со специалистами по ИБ или включать в состав рабочей группы представителей отдела информационной безопасности;

• На регулярной основе разрабатывать положения, процедуры, инструкции и прочие документы, дополняющие политику ИБ (инструкция по предоставлению доступа к сети интернет, инструкция по предоставлению доступа в помещения с ограниченным доступом, инструкции по работе с информационными системами компании и т.п.);

• Не реже, чем раз в квартал, пересматривать политику ИБ и прочие документы по ИБ с целью их актуализации.

Следует отметить, что в крупных предприятиях и организациях реализация всех этапов процесса внедрения политики информационной безопасности — от согласования до сертификации и аттестации — является сложной задачей. Однако целесообразность этого решения помогает преодолеть все преграды в случае, если все работы в разработке и внедрению политики ИБ выполняются по специализированному алгоритму, учитывающему все необходимые критерии разработки, стандарты и процедуры. При этом последовательность, количество операций и действий такого алгоритма в каждом случае может быть индивидуальным и иметь отличия от прототипов, рекомендованных стандартами по ИБ, поскольку необходимо учитывать все технические, юридические и административные аспекты конкретного предприятия или организации. На рисунке 10 представлен вариант алгоритма разработки политики ИБ.

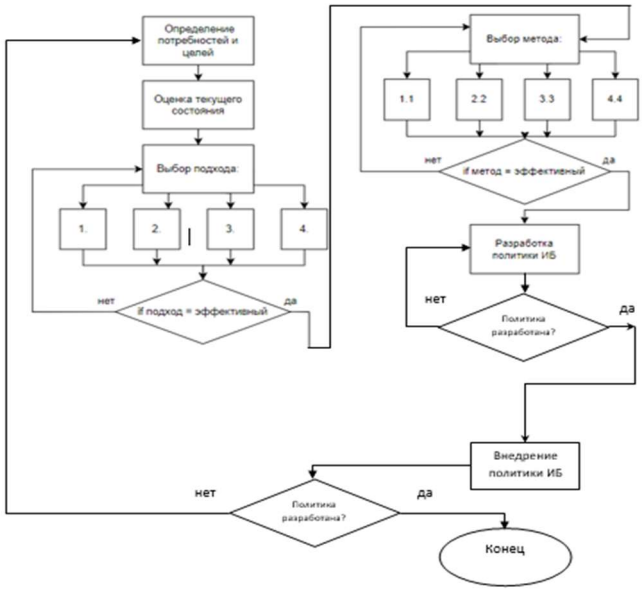

Рисунок 10 — Алгоритм разработки политики ИБ

Таким образом, учитывая особенности функционирования алгоритма разработки политики ИБ при выборе инструментов и технологий для разработки политики информационной безопасности, важно учитывать следующие аспекты:

1. Требования организации: определить основные угрозы и риски ИБ, с которыми сталкивается организация.

2. Масштабируемость: выбирать решения реализации ИС и ее подсистем, которые могут быть легко масштабированы по мере роста организации.

3. Совместимость: обеспечить интеграцию выбранных инструментов с существующими системами и процессами.

4. Обучение персонала: инвестировать в обучение сотрудников для эффективного использования выбранных технологий и решений.

Таким образом, исходя из вышеизложенного, рекомендуется:

- Для защиты сети использовать межсетевые экраны для контроля внешнего трафика и IDS/IPS для детекции и предотвращения сложных атак.

- Для шифрования данных использовать AES и SSL/TLS для обеспечения защищенных соединений.

- Для управления инцидентами внедрять SIEM для централизованного сбора и анализа данных и организовать SOC для круглосуточного мониторинга и реагирования на угрозы. В таблице 2 представлен сравнительный анализ преимуществ и недостатков, реализующих функциональные требования политики ИБ.

Таблица 2. Сравнение технологий, реализующих функциональные требования политики ИБ

Технология	**Преимущества**	**Недостатки**
	Предотвращение утечек данных, мониторинг активности пользователей	Высокая стоимость, сложность внедрения
	Сбор и анализ информации о событиях безопасности, обнаружение угроз	Требует значительных ресурсов для установки и обслуживания
Антивирусы	Защита от вредоносного ПО, простота использования	Ограниченная защита от новых и сложных угроз
	Обнаружение и предотвращение вторжений, анализ сетевого трафика	Высокий уровень ложных срабатываний, требуются высококвалифицированные специалисты для настройки

Таким образом, говоря о защите информации в целом, можно говорить о том, что защита информации как гарантия безопасности относится к задачам государства. Но следует отметить, что и пользователи, и владельцы различных ИС способны проводить мероприятия по повышению информационной безопасности ИС и защите информации в целом. Для этого, как правило, следует применять стандартные меры, такие как политика разграничения доступа к ресурсам критически важных ИС, ограничение доступа к информационным ресурсам, имеющим ценность, защита внешнего и внутреннего периметра сети ИС, и многие другие решения для защити информации и самой ИС. Все эти меры являются составной частью единого комплексного решения по обеспечению ИБ, во главе которого стоит политика ИБ. Именно поэтому успех в обеспечении защиты информации от воздействия киберугроз может принести только комплексный подход, сочетающий в себе уровни, входящие в состав политики ИБ – процедурный, законодательный, программно-технический. Исходя из этого, необходимо понимать, что адаптация традиционных мер – сетевых решений, повышение качества сбора оперативной информации, моделирование угроз, повышение ответственности — также расширяет границы «безопасного периметра» и создает условия для эффективного и безопасного использования информации в режиме реального времени. Подводя итоги

исследования, проводимого в рамках данной работы, можно говорить о том, что были детально рассмотрены этапы разработки, различные методы и подходы к формированию политики информационной безопасности, включая нормативный, рисковый, проактивный и реактивный подходы. Был выполнен сравнительный анализ указанных подходов, выявлены их преимущества и недостатки. На основании полученных данных предложены рекомендации по применению комбинированного подхода для создания эффективной политики ИБ как компонента системы защиты информации, обеспечивающей всестороннюю безопасность организации, предложен вариант алгоритма разработки политики ИБ.

Литература

1. ISO/IEC 27001-2005. Information technology - Security techniques - Information security management systems - Requirements.
2. IT-Enigma.ru
3. LanAgent.ru
4. https://falcongaze.com/ru/pressroom/publications/articles/%D0%BF%D0%BE%D0%BB%D0%B8%D1%82%D0%B8%D0%BA%D0%B0-%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9-%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8.html
5. https://habr.com/ru/articles/174489/
6. ISO/IEC 17799-2005. Information technology - Security techniques - Code of practice for information security management.
7. ГОСТ Р ИСО/МЭК 15408. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.
8. Azone-IT.ru
9. https://lanagent.ru/
10. https://www.komset.ru/informatsiya-o-kompanii/articles/zaschita-informatsii-v-lokalnykh-setyakh
11. https://chatgpt.com/
12. https://app.diagrams.net/
13. https://ovfd.zdrav76.ru/?page_id=848
14. https://www.expocentr.ru/ru/articles-of-exhibitions/17039/