УДК 004.056.5

*С. В. Корякин*[1,2]
[1]*Старший преподаватель, Институт информационных технологий КГТУ им. И.Раззакова*
[2] *Научный сотрудник, Институт машиноведения автоматики и геомеханики НАН КР*
*Салиев А.Б.*
*д.ф.-м.н., профессор, Институт информационных технологий КГТУ им. И.Раззакова*
*Салиев С.М., salievsamat0@gmail.com*
*Студент гр. ИБ-2-22, Институт информационных технологий КГТУ им. И.Раззакова*
*Верзунов С.Н.*
*Ведущий научный сотрудник, Институт машиноведения, автоматики и геомеханики НАН КР, verzunov@hotmail.com*

# АНАЛИТИЧЕСКИЙ ОБЗОР ОСНОВНЫХ НАПРАВЛЕНИЙ, ПРИНЦИПОВ И МЕТОДОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АИС

В статье рассматриваются основные направления, принципы и методы обеспечения информационной безопасности автоматизированных информационных систем (АИС). Основное внимание уделяется анализу возможных угроз и уязвимостей информационных систем, а также организационным, техническим, правовым и процедурным мерам по защите информации. Рассматриваются принципы конфиденциальности, целостности, доступности, аутентичности и неотказуемости как фундаментальные основы информационной безопасности. Производится обзор различных инструментов защиты, включая криптографические средства, системы управления доступом, антивирусные программы, системы обнаружения и предотвращения вторжений, а также резервное копирование и восстановление данных. Таким образом, статья направлена на систематизацию существующих знаний и методов для обеспечения информационной безопасности АИС, что позволит улучшить защиту информационных систем предприятий и организаций от различных угроз и атак.

***Ключевые слова:*** информационная безопасность, аудит, меры, IDS/IPS, DLP, SIEM, автоматизированная информационная система, методы, инцидент, шифрование, GDPR, ISO/IEC 27001

В условиях стремительного роста объемов информации и увеличения сложности автоматизированных информационных систем (АИС) вопросы обеспечения их безопасности становятся в особенности важными для предприятий и организаций. Обеспечение информационной безопасности АИС направлено на защиту данных от несанкционированного доступа, изменения, уничтожения и других угроз, которые могут привести к значительным как финансовым, так и репутационным потерям.

Несмотря на значительные усилия и внедрение современных технологий защиты, сохраняются многочисленные уязвимости, которые могут быть использованы злоумышленниками для несанкционированного доступа, изменения или уничтожения данных. Проблема заключается в необходимости комплексного подхода к обеспечению информационной безопасности АИС, включающего организационные, технические, правовые и процедурные меры, которые могли бы эффективно противодействовать как существующим, так и новым угрозам.

Основные аспекты проблемы включают:

- Недостаточную осведомленность и ошибки пользователей, являющиеся одной из главных причин инцидентов безопасности.
- Использование устаревшего программного обеспечения и оборудования, не поддерживающего современные стандарты защиты.

- Неполное или некорректное внедрение политик управления доступом и мониторинга активности пользователей.
- Наличие сложных и разнообразных угроз, требующих применения многослойных и адаптивных методов защиты.

Для решения данной проблемы необходимо систематизировать знания о существующих угрозах и уязвимостях, а также проанализировать и оценить эффективность различных подходов и технологий обеспечения информационной безопасности.[1]

Считается, что под направлениями обеспечения информационной безопасности автоматизированных информационных систем (АИС) понимаются основные области деятельности и подходы, направленные на защиту информации и систем от различных угроз. Эти направления охватывают широкий спектр мер и стратегий, включающих как технические, так и организационные аспекты. Основные направления обеспечения информационной безопасности АИС включают:

1. *Организационные меры:*
    - *Политики и процедуры*. Разработка и внедрение корпоративных политик и процедур по информационной безопасности, включая правила использования информационных систем, управления доступом и реагирования на инциденты.
    - *Обучение и осведомленность*. Регулярное обучение сотрудников и повышение их осведомленности о правилах информационной безопасности.
    - *Аудит и мониторинг*. Проведение регулярных аудитов и мониторинга для оценки текущего состояния безопасности и выявления потенциальных угроз.
2. *Технические меры[2]:*
    - *Шифрование*. Использование криптографических методов для защиты данных при передаче и хранении.
    - *Системы управления доступом*. Внедрение механизмов аутентификации и авторизации, таких как многофакторная аутентификация и ролевое управление доступом.
    - *Защитное ПО*. Установка и обновление антивирусных программ, брандмауэров и систем обнаружения и предотвращения вторжений (IDS/IPS).
3. *Правовые меры [3*]:
    - *Соответствие нормативным требованиям*. Обеспечение соответствия законодательным и нормативным требованиям в области информационной безопасности, таким как GDPR, ISO/IEC 27001 и другие.
    - *Договоры и соглашения*. Разработка юридических документов, включая соглашения о конфиденциальности и контракты с поставщиками услуг.
4. *Процедурные меры:*
    - *Реагирование на инциденты*. Разработка и внедрение процедур реагирования на инциденты информационной безопасности, включая план действий при утечках данных и кибератаках.
    - *Управление рисками*. Оценка и управление рисками, связанными с информационной безопасностью, включая идентификацию, анализ и принятие мер по минимизации рисков.
    - *Резервное копирование и восстановление*. Обеспечение регулярного резервного копирования данных и разработка планов восстановления после сбоев.

5. *Физические меры [4]:*
   - *Контроль доступа к помещениям*. Обеспечение физической безопасности серверных помещений и рабочих мест.
   - *Защита оборудования*. Использование сейфов, замков и других средств для защиты оборудования от кражи и несанкционированного доступа.

Эти направления взаимосвязаны и дополняют друг друга, создавая многослойную защиту, которая способна противостоять современным угрозам информационной безопасности (рис.1).


Рисунок 1 – Обобщенная блок-схема направлений обеспечения безопасности

***Исходя из рисунка 1, предлагается выделить следующие принципы и методы, которые необходимо использовать в процессах обеспечения безопасности АИС, под которыми*** понимаются базовые правила и концепции, служащие основой для разработки и внедрения мер по защите информации и систем от различных киберугроз и направленных на создание комплексной и эффективной системы защиты. Основные принципы обеспечения информационной безопасности АИС включают [5]:

1. ***Конфиденциальность:***
   - Обеспечение доступа к информации только тем пользователям, которые имеют на это разрешение.
   - Использование методов шифрования и контроля доступа для защиты данных от несанкционированного просмотра.[5]
2. ***Целостность:***
   - Защита данных от несанкционированного изменения или уничтожения.
   - Применение методов контроля целостности данных, таких как контрольные суммы и цифровые подписи.[5]
3. ***Доступность:***

- Обеспечение возможности доступа к информации и системам для уполномоченных пользователей в любое необходимое время.
- Защита от отказов в обслуживании (DoS/DDoS атаки) и обеспечение устойчивости системы к сбоям и отказам.[5]

4. ***Аутентичность:***
   - Гарантия подлинности и достоверности источника данных.
   - Использование методов аутентификации, таких как пароли, биометрические данные и цифровые сертификаты.
5. ***Неотказуемость***:
   - Обеспечение невозможности отрицания факта отправки или получения информации.
   - Использование цифровых подписей и журналов аудита для подтверждения действий пользователей.[5]
6. ***Разделение обязанностей***:
   - Разделение критических задач и функций между несколькими сотрудниками для уменьшения риска внутреннего мошенничества и ошибок.
   - Введение различных уровней доступа и прав для выполнения различных операций.
7. ***Минимизация привилегий:***
   - Предоставление пользователям минимально необходимого уровня доступа для выполнения их задач.
   - Регулярный пересмотр и ограничение прав доступа на основе текущих задач и ролей.
8. ***Мониторинг и аудит:***
   - Постоянное наблюдение за действиями пользователей и системными событиями.
   - Ведение журналов аудита и проведение регулярных проверок для выявления и анализа подозрительной активности.[5,8]
9. ***Управление рисками:***
   - Оценка и управление рисками, связанными с информационной безопасностью.
   - Идентификация, анализ и принятие мер по минимизации потенциальных угроз и уязвимостей.
10. ***Постоянное улучшение:***
    - Регулярное обновление и совершенствование мер безопасности в ответ на новые угрозы и технологии.
    - Проведение обучения и повышения осведомленности сотрудников, а также тестирование и обновление защитных систем.

Эти принципы формируют основу для создания и поддержания надежной системы информационной безопасности, позволяя эффективно защищать данные и обеспечивать стабильную работу автоматизированных информационных систем (рис. 2).

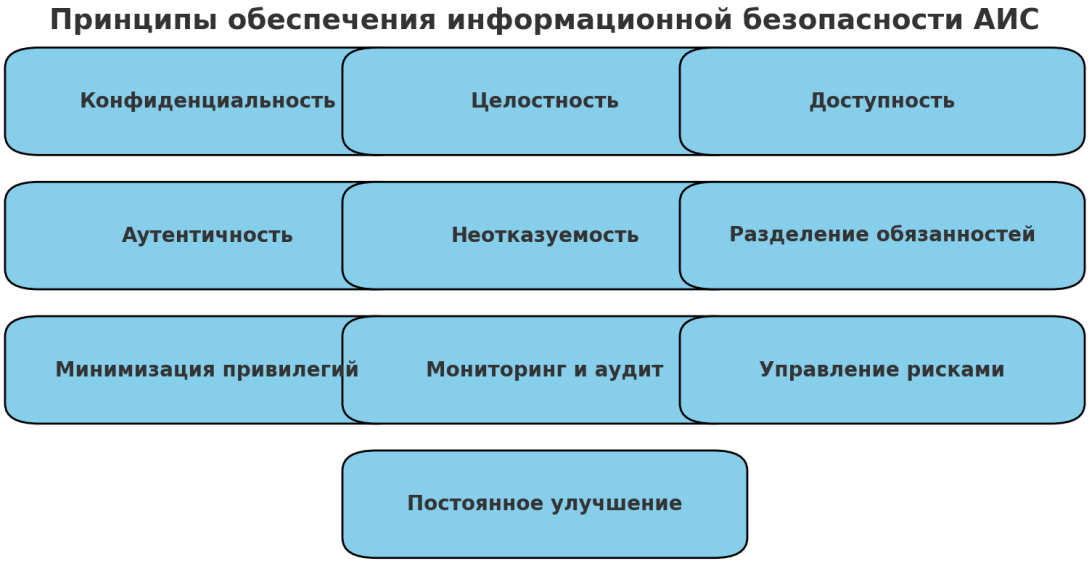


Рисунок 2 – Принципы обеспечения информационной безопасности АИС

Под методами обеспечения информационной безопасности автоматизированных информационных систем (АИС) понимаются конкретные средства, технологии и процедуры, используемые для защиты информации и систем от различных угроз. Эти методы включают как технические, так и организационные меры, направленные на предотвращение, обнаружение и реагирование на инциденты безопасности.[5] Основные методы обеспечения информационной безопасности АИС включают:

1. ***Криптографические методы:***
   - ***Шифрование данных.*** Применение симметричных и асимметричных алгоритмов шифрования для защиты данных при передаче и хранении.
   - ***Цифровые подписи***. Использование цифровых подписей для обеспечения целостности и аутентичности данных.
   - ***Хеширование.*** Применение хеш-функций для проверки целостности данных и хранения паролей.[6]
2. ***Методы аутентификации и авторизации:***
   - ***Парольная аутентификация***. Использование сложных паролей для подтверждения личности пользователя.
   - ***Многофакторная аутентификация (MFA)***. Применение нескольких факторов (пароль, смс-код, биометрия) для повышения надежности аутентификации.
   - ***Ролевая и атрибутивная модель управления доступом (RBAC/ABAC)***. Назначение прав доступа на основе ролей и атрибутов пользователей.[6]
3. ***Средства обнаружения и предотвращения вторжений (IDS/IPS):***
   - ***Системы обнаружения вторжений (IDS)***. Мониторинг сетевого трафика и активности систем для выявления подозрительных действий.
   - ***Системы предотвращения вторжений (IPS).*** Автоматическое принятие мер для блокировки или ограничения вредоносной активности.
4. ***Антивирусные и антишпионские программы:***

- ***Антивирусное ПО***. Использование программ для обнаружения и удаления вредоносного ПО (вирусы, трояны, черви).
- ***Антишпионское ПО.*** Применение средств для обнаружения и удаления шпионского ПО.

5. ***Методы защиты сетей:***
   - ***Брандмауэры (Firewall)***. Установка межсетевых экранов для контроля и фильтрации сетевого трафика.
   - ***Виртуальные частные сети (VPN)***. Использование технологий для создания защищенных каналов связи через Интернет.
6. ***Методы резервного копирования и восстановления данных:***
   - ***Резервное копирование.*** Регулярное создание копий данных для предотвращения их потери в случае сбоя или атаки.
   - ***Планы восстановления после сбоев.*** Разработка и внедрение процедур для быстрого восстановления работы систем после инцидентов.
7. ***Методы мониторинга и аудита:***
   - ***Журналирование.*** Ведение журналов аудита для фиксации всех значимых действий в системе.
   - ***Анализ логов***. Регулярный анализ журналов для выявления аномалий и инцидентов безопасности.[7]
8. ***Методы управления уязвимостями:***
   - ***Патч-менеджмент.*** Обновление программного обеспечения для устранения известных уязвимостей.
   - ***Пентест (тестирование на проникновение).*** Проведение тестов на проникновение для выявления и устранения уязвимостей.
9. ***Обучение и повышение осведомленности:***
   - ***Тренинги по безопасности***. Регулярное обучение сотрудников правилам информационной безопасности.
   - ***Фишинг-тесты.*** Проведение тестов на осведомленность сотрудников о фишинговых атаках.[8]
10. ***Методы реагирования на инциденты:***
    - ***Планы реагирования на инциденты***. Разработка и внедрение процедур для быстрого и эффективного реагирования на инциденты.
    - ***Анализ инцидентов***. Проведение расследований инцидентов для выявления причин и разработки мер по предотвращению повторения.

Из перечисленного выше следует, что использование указанных методов при построении подсистем защиты АИС информации позволяет обеспечить многослойную защиту информации и систем, создавая комплексную подсистему безопасности, способную эффективно противостоять современным киберугрозам (рис.3).


Рисунок 3 – Методы обеспечения информационной безопасности

**Обзор современных инструментов и технологий**

Таким образом следует понимать, что в современном мире, где информация играет все более важную роль, обеспечение информационной безопасности (ИБ) автоматизированных информационных систем (АИС) становится критически важной задачей. С ростом использования информационных технологий и ценности данных киберугрозы становятся все более изощренными. Для защиты АИС от этих угроз необходимо использовать широкий спектр современных инструментов и технологий, таких как:

***1. Системы контроля доступа (СКД):***

- ***Active Directory.*** Централизованная система управления доступом, позволяющая управлять правами пользователей на доступ к ресурсам сети.
- ***Kerberos.*** Протокол аутентификации, обеспечивающий безопасный доступ к ресурсам сети.
- ***SAML (Security Assertion Markup Language).*** Протокол обмена аутентификационной информацией между различными системами.
- ***SSO (Single Sign-On).*** Единый вход в систему, позволяющий пользователям аутентифицироваться один раз и получать доступ к нескольким системам.
- ***Biometric authentication.*** Использование биометрических данных (отпечатки пальцев, распознавание лица) для аутентификации пользователей [9].

В таблице 1 приведен сравнительный анализ характеристик СКД.

Таблица 1– Сравнительный анализ характеристик СКД

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| Active Directory | Широкий набор функций, включая управление пользователями, группами, правами доступа и политиками безопасности | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, используемая во многих крупных организациях. | Может быть сложной для настройки и управления | Бесплатно для Windows Server |
| Kerberos | Простой и надежный протокол аутентификации. | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, используемая во многих крупных организациях. | Может быть сложной для настройки и управления | Бесплатно |
| SAML | Стандартный протокол обмена аутентификационной информацией между различными системами | Позволяет использовать единый вход в систему для нескольких систем | Хорошо масштабируется для больших организаций | Надежный стандарт, поддерживаемый многими системами | Может быть сложной для настройки и управления | Стоимость зависит от конкретной реализации |

***2. Антивирусное программное обеспечение (АПО) [8]:***

- ***Kaspersky Internet Security.*** Комплексное антивирусное решение, защищающее от вирусов, троянов, червей, шпионских программ и других угроз.
- ***Eset NOD32 Antivirus.*** Антивирусное решение, известное своей эффективностью и низким потреблением системных ресурсов.
- ***Bitdefender Antivirus Plus.*** Антивирусное решение, предлагающее широкий спектр функций.
- ***Avast Antivirus.*** Бесплатное антивирусное решение, обеспечивающее базовую защиту от вирусов и других угроз.
- ***AVG Antivirus.*** Еще одно бесплатное антивирусное решение, предлагающее различные платные функции.

В таблице 2 приведен сравнительный анализ характеристик АПО.

Таблица 2– Сравнительный анализ характеристик АПО

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| Kaspersky Internet Security | Широкий набор функций, включая защиту от вирусов, троянов, | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Легко использовать | Платная |

| | | | | | | |
|---|---|---|---|---|---|---|
| | червей, шпионских программ и других угроз | | | | | |
| Eset NOD32 Antivirus | Эффективная защита от вирусов и других угроз | Низкое потребление системных ресурсов | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Легко использовать | Платная |

**3.** ***Межсетевые экраны (МЭ) [16]:***

- ***Cisco Firepower Management Center*.** Комплексная система межсетевой безопасности, включающая в себя межсетевой экран, систему обнаружения и предотвращения вторжений (IDS/IPS) и другие функции.
- ***Palo Alto Networks PAN-OS*.** Межсетевой экран нового поколения, предлагающий широкий спектр функций, включая защиту от APT-атак и URL-фильтрацию.
- ***Fortinet FortiGate.*** Межсетевой экран, известный своей надежностью и высокой производительностью.
- ***SonicWall NSv.*** Виртуальный межсетевой экран, удобный для развертывания в облачных средах.
- ***Checkpoint SandBlast Network.*** Межсетевой экран нового поколения, использующий технологии песочницы для защиты от неизвестных угроз.

В таблице 3 приведен сравнительный анализ МЭ.

Таблица 3– Сравнительный анализ МЭ

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| Cisco Firepower Management Center | Комплексная система межсетевой безопасности, включающая в себя межсетевой экран, систему обнаружения и предотвращения вторжений (IDS/IPS) и другие функции | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, используемая во многих крупных организациях | Может быть сложной для настройки и управления | Платная |
| Palo Alto Networks PAN-OS | Межсетевой экран нового поколения, предлагающий широкий спектр функций, включая защиту от APT-атак и URL-фильтрацию | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Платная |
| Fortinet FortiGate | Межсетевой экран, | Высокая производительн | Хорошо масштабируетс | Надежная система, | Легко использоват | Платная |

| | | | | | | |
|---|---|---|---|---|---|---|
| | известный своей надежностью и высокой производительностью | ость | я для больших организаций | хорошо зарекомендовавшая себя | ь | |

***4. Системы обнаружения вторжений (СОВ) [16]:***

- ***Snort.*** Open-source система обнаружения вторжений, использующая сигнатурный анализ и методы статистического анализа трафика.
- ***Suricata.*** Еще одна open-source система обнаружения вторжений, основанная на Snort.
- ***Deepwatch Network Security.*** Коммерческая система обнаружения вторжений, использующая машинное обучение для выявления неизвестных угроз.
- ***McAfee Network Security Platform.*** Комплексная система сетевой безопасности, включающая в себя IDS/IPS, межсетевой экран и другие функции.
- ***Cisco Security Center.*** Комплексная система безопасности, включающая в себя IDS/IPS, межсетевой экран, SIEM и другие функции.

В таблице 4 приведен сравнительный анализ СОВ.

Таблица 4 – Сравнительный анализ СОВ

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| Snort | Open-source система обнаружения вторжений, использующая сигнатурный анализ и методы статистического анализа трафика | Средняя производительность | Хорошо масштабируется для больших организаций | Бесплатная система, но может требовать значительных ресурсов для работы | Может быть сложной для настройки и управления | Бесплатно |
| Cisco Security Center | Комплексная система безопасности, включающая в себя IDS/IPS, межсетевой экран, SIEM и другие функции | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Платная |

**5***. Системы предотвращения вторжений (СПВ) [16]:*

- ***Cisco Firepower NGIPS.*** Система предотвращения вторжений нового поколения, основанная на Cisco Firepower Management Center.
- ***Palo Alto Networks PAN-OS.*** Система предотвращения вторжений, интегрированная с межсетевым экраном PAN-OS.
- ***Fortinet FortiGate.*** Система предотвращения вторжений, интегрированная с межсетевым экраном FortiGate.
- ***SonicWall NSv.*** Виртуальная система предотвращения вторжений, удобная для развертывания в облачных средах.

- ***Checkpoint SandBlast Network*.** Система предотвращения вторжений нового поколения, использующая технологии песочницы для защиты от неизвестных угроз.

В таблице 5 приведен сравнительный анализ СПВ.

Таблица 5 – Сравнительный анализ СПВ

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| Cisco Firepower NGIPS | Система предотвращения вторжений нового поколения, основанная на Cisco Firepower Management Center | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, используемая во многих крупных организациях | Может быть сложной для настройки и управления | Платная |
| Fortinet FortiGate | Система предотвращения вторжений, интегрированная с межсетевым экраном FortiGate | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Легко использовать | Платная |

**6.** ***Системы шифрования [9]:***

- ***PGP (Pretty Good Privacy).*** Open-source система шифрования, использующая криптографию с открытым ключом.
- ***GPG (GNU Privacy Guard).*** Свободная реализация PGP.
- ***VeraCrypt.*** Бесплатная программа шифрования, позволяющая шифровать файлы, диски и разделы диска.
- ***BitLocker.*** Система шифрования дисков, встроенная в Windows.
- ***FileVault 2*.** Система шифрования дисков, встроенная в macOS.

В таблице 6 приведен сравнительный анализ PGP.

Таблица 6– Сравнительный анализ PGP

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| PGP | Open-source система шифрования, использующая криптографию с открытым ключом | Средняя производительность | Хорошо масштабируется для больших организаций | Надежная система, используемая во многих крупных организациях | Может быть сложной для использования для неискушенных пользователей | Бесплатно |
| GPG | Свободная реализация PGP | Средняя производительно | Хорошо масштабируетс | Надежная система, | Может быть сложной | Бесплатно |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | сть | я для больших организаций | используемая во многих крупных организациях | для использования для неискушенных пользователей | |
| VeraCrypt | Бесплатная программа шифрования, позволяющая шифровать файлы, диски и разделы диска | Средняя производительность | Хорошо масштабируется для больших организаций. | Надежная система, хорошо зарекомендовавшая себя | Легко использовать | Бесплатно |

**7.** ***Системы резервного копирования [8]:***

- ***Veeam Backup & Replication.*** Коммерческая система резервного копирования, предлагающая широкий спектр функций.
- ***Acronis Backup & Recovery.*** Еще одна коммерческая система резервного копирования, известная своей простотой использования.
- ***CrashPlan.*** Облачная система резервного копирования, позволяющая хранить резервные копии данных в защищенном дата-центре.
- ***UrBackup.*** Open-source система резервного копирования, предлагающая широкий спектр функций.
- ***Backupper.*** Бесплатная программа резервного копирования, позволяющая создавать резервные копии файлов, дисков и разделов диска.
- ***Duplicati.*** Бесплатная программа резервного копирования с открытым исходным кодом, позволяющая создавать резервные копии данных в локальном хранилище или в облаке.

В таблице 7 приведен сравнительный анализ Системы резервного копирования.

Таблица 7 – Сравнительный анализ систем резервного копирования

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| Veeam Backup & Replication | Коммерческая система резервного копирования, предлагающая широкий спектр функций | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Платная |
| Acronis Backup & Recovery | Еще одна коммерческая система резервного копирования, известная своей простотой использования | Средняя производительность | Хорошо масштабируется для средних и крупных организаций | Надежная система, хорошо зарекомендовавшая себя | Легко использовать | Платная |

***8. Системы управления информационной безопасностью (СУИБ):***

- ***IBM Security QRadar.*** Коммерческая СУИБ, предлагающая широкий спектр функций, включая мониторинг событий безопасности, анализ журналов и реагирование на инциденты.
- ***McAfee ePolicy Orchestrator.*** Коммерческая СУИБ, известная своей масштабируемостью и надежностью.
- ***LogRhythm SIEM.*** Коммерческая СУИБ, предлагающая функции мониторинга событий безопасности, анализа журналов и реагирования на инциденты.
- ***AlienVault USM Anywhere.*** Облачная СУИБ, удобная для использования малыми и средними предприятиями.
- ***OSSEC.*** Open-source СУИБ, предлагающая базовые функции мониторинга событий безопасности и анализа журналов.

В таблице 8 приведен сравнительный анализ СУИБ.

Таблица 8 — Сравнительный анализ СУИБ

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| IBM Security QRadar | Коммерческая СУИБ, предлагающая широкий спектр функций, включая мониторинг событий безопасности, анализ журналов и реагирование на инциденты | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, используемая во многих крупных организациях | Может быть сложной для настройки и управления | Платная |
| McAfee ePolicy Orchestrator | Коммерческая СУИБ, известная своей масштабируемостью и надежностью | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Платная |
| OSSEC | Open-source СУИБ, предлагающая базовые функции мониторинга событий безопасности и анализа журналов | Средняя производительность | Хорошо масштабируется для организаций всех размеров | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Бесплатно. |

***9. SIEM-системы [9]:***

- ***Splunk.*** Коммерческая SIEM-система, предлагающая широкий спектр функций, включая сбор и анализ журналов, мониторинг событий безопасности и реагирование на инциденты.
- ***ArcSight Investigator*.** Коммерческая SIEM-система, известная своей мощностью и масштабируемостью.
- ***LogRhythm SIEM.*** Коммерческая SIEM-система, предлагающая функции мониторинга событий безопасности, анализа журналов и реагирования на инциденты.
- ***Elastic Stack (ELK).*** Open-source SIEM-система, основанная на Elasticsearch, Logstash и Kibana.
- ***Graylog*.** Open-source SIEM-система, предлагающая базовые функции сбора и анализа журналов.

В таблице 9 приведен сравнительный анализ SIEM-систем.

Таблица 9 — Сравнительный анализ SIEM-систем

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| LogRhythm SIEM | Коммерческая SIEM-система, предлагающая функции сбора и анализа журналов, мониторинга событий безопасности и реагирования на инциденты | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Платная |
| Graylog | Open-source SIEM-система, предлагающая базовые функции сбора и анализа журналов | Средняя производительность | Хорошо масштабируется для организаций всех размеров | Надежная система, хорошо зарекомендовавшая себя | Легко использовать | Бесплатно |
| Splunk | Коммерческая SIEM-система, предлагающая широкий спектр функций, включая сбор и анализ журналов, мониторинг событий | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, используемая во многих крупных организациях | Может быть сложной для настройки и управления | Платная |

| | | | | | | |
|---|---|---|---|---|---|---|
| | безопасности и реагирование на инциденты | | | | | |

***10. DLP-системы** [9]**:***

- ***McAfee DLP Suite.*** Коммерческая DLP-система, предлагающая широкий спектр функций, включая контроль конфиденциальной информации, шифрование данных и предотвращение утечек.
- ***Symantec DLP Suite.*** Коммерческая DLP-система, известная своей эффективностью и точностью.
- ***Cisco Secure Content Manager.*** Коммерческая DLP-система, интегрированная с другими решениями Cisco по безопасности.
- ***Digital Guardian DLP.*** Коммерческая DLP-система, предлагающая функции контроля конфиденциальной информации, шифрования данных и предотвращения утечек.
- ***Irius Risk Manager.*** Open-source DLP-система, предлагающая базовые функции контроля конфиденциальной информации.

В таблице 10 приведен сравнительный анализ DLP-системы.

Таблица 10 — Сравнительный анализ DLP-системы

| **Технология/Инструмент** | **Функциональность** | **Производительность** | **Масштабируемость** | **Надежность** | **Простота использования** | **Стоимость** |
|---|---|---|---|---|---|---|
| McAfee DLP Suite | Коммерческая DLP-система, предлагающая широкий спектр функций, включая контроль конфиденциальной информации, шифрование данных и предотвращение утечек | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Платная |
| Symantec DLP Suite | Коммерческая DLP-система, известная своей эффективностью и точностью | Высокая производительность | Хорошо масштабируется для больших организаций | Надежная система, хорошо зарекомендовавшая себя | Может быть сложной для настройки и управления | Платная |
| Cisco Secure Content Manager | Коммерческая DLP-система, | Высокая производительность | Хорошо масштабируется для больших | Надежная система, хорошо | Может быть сложной | Платная |

| | | | | | | |
|---|---|---|---|---|---|---|
| | интегрированная с другими решениями Cisco по безопасности | | организаций | зарекомендовавшая себя | для настройки и управления | |

Помимо перечисленных технологий и инструментов, существует множество других решений, которые могут быть использованы для обеспечения информационной безопасности АИС, при этом выбор конкретных технологий и инструментов должен зависеть от: потребностей организации, уровня ее рисков, бюджета, кадрового обеспечения. Также важно, чтобы все используемые технологии и инструменты были интегрированы друг с другом и работали в единой системе, поскольку обеспечение информационной безопасности АИС – это непрерывный процесс, который требует постоянного внимания и усилий.

Именно поэтому предлагается регулярно проводить организационные и технические мероприятия такие, как оценка рисков, обновление технологий и инструментов, обучение персонала, тестирование системы безопасности, не забывая о том, что только комплексный подход к обеспечению информационной безопасности позволит защитить АИС от киберугроз.

Таким образом, на основе проведенного анализа следует отметить, что при построении системы защиты информации для АИС важно учитывать множество факторов, включая специфику бизнеса, объем и чувствительность данных, а также существующие угрозы и уязвимости. Именно поэтому предлагаются следующие рекомендации по выбору наиболее подходящих инструментов для различных аспектов информационной безопасности:

1. **Управление доступом и аутентификация**

**Рекомендации:**

**Microsoft Active Directory (AD)**. Для централизованного управления учетными записями пользователей и их правами доступа.

**Okta или Azure AD**. Для реализации многофакторной аутентификации (MFA) и единого входа (SSO).

**Преимущества:**

Централизованное управление пользователями и их правами доступа; повышенная безопасность за счет многофакторной аутентификации.

2. **Защита сети**

**Рекомендации:**

**Cisco ASA или Palo Alto Networks**. Для защиты периметра сети с помощью межсетевых экранов и систем предотвращения вторжений (IDS/IPS);

**Snort**: Для глубокого анализа трафика и обнаружения угроз.

**Преимущества:**

Эффективная защита от внешних атак и несанкционированного доступа; возможность обнаружения и предотвращения подозрительной активности в реальном времени.

3. **Шифрование данных**

**Рекомендации:**

**BitLocker**. Для шифрования данных на локальных дисках и съемных носителях.

**OpenSSL**. Для обеспечения безопасности передачи данных через Интернет с использованием SSL/TLS.

**Преимущества:**

Защита данных на устройствах и в процессе их передачи; поддержка высоких стандартов безопасности и совместимость с различными системами[10].

4. **Антивирусное ПО**

**Рекомендации:**

**Symantec Endpoint Protection или McAfee Total Protection**. Для защиты от вирусов, троянов и других вредоносных программ.

**Malwarebytes**. Для дополнительной защиты и удаления вредоносного ПО.

**Преимущества:**

Эффективное обнаружение и удаление вредоносных программ; постоянное обновление баз данных угроз для защиты от новых вирусов.

5. **Мониторинг и управление инцидентами**

**Рекомендации:**

**Splunk или IBM QRadar**. Для централизованного сбора, анализа и корреляции событий безопасности (SIEM).

**Archer от RSA**. Для управления рисками и инцидентами, а также обеспечения соответствия нормативным требованиям.

**Преимущества:**

Обеспечение видимости и контроля над событиями безопасности в реальном времени; автоматизация процессов обнаружения, анализа и реагирования на инциденты.

6. **Резервное копирование и восстановление данных**

**Рекомендации:**

**Veeam Backup & Replication**. Для регулярного создания резервных копий данных и их восстановления в случае утраты.

**Acronis Backup**. Для обеспечения непрерывности бизнеса и защиты данных от сбоев и катастроф.

**Преимущества:**

Надежное резервное копирование и быстрое восстановление данных; защита от потерь данных из-за аппаратных сбоев или кибератак.

7. **Защита от утечек данных (DLP)**

**Рекомендации:**

**Symantec Data Loss Prevention**. Для мониторинга и предотвращения утечек конфиденциальной информации.

**Forcepoint DLP**. Для контроля и защиты данных как на уровне конечных точек, так и при передаче через сеть.

**Преимущества:**

Предотвращение несанкционированного распространения конфиденциальной информации, поддержка различных политик и правил для защиты данных[11].

Таким образом, в рамках проведенного аналитического обзора были выявлены ключевые направления, принципы и методы защиты информации, а также проведена оценка современных инструментов и технологий, используемых для формирования надежной системы безопасности. Информационная безопасность в современных условиях требует применения комплексного подхода, включающего взаимосвязанные организационные и технические меры, которые в совокупности обеспечивают минимизацию рисков и предотвращение инцидентов, связанных с несанкционированным доступом или нарушением целостности данных.

Организационные методы, такие как разработка и внедрение политик безопасности, управление правами доступа, а также обучение сотрудников основам информационной безопасности, создают базовые условия для обеспечения защищенности на уровне всей организации. Эти меры способствуют формированию устойчивой системы управления рисками, направленной на минимизацию вероятности человеческих ошибок, а также обеспечивают соответствие установленным нормативам и стандартам в сфере информационной безопасности.

Технические средства представляют собой основу защиты IT-инфраструктуры. К ним относятся межсетевые экраны, системы обнаружения и предотвращения вторжений (IDS/IPS), антивирусные программы, технологии шифрования данных, а также решения для резервного копирования информации. Указанные инструменты обеспечивают многоуровневую защиту, способную нейтрализовать широкий спектр угроз и уменьшить потенциальные последствия инцидентов информационной безопасности.

Таким образом, формирование эффективной системы защиты информации возможно лишь при интеграции организационных и технических мер, что позволяет создать устойчивую и адаптивную IT-инфраструктуру, способную противостоять современным киберугрозам. Данный подход обеспечивает комплексное управление рисками, повышая надежность системы безопасности и снижая уязвимость информационных ресурсов.

**Литература:**


1. Smart-Soft. Защита информации в автоматизированных системах. URL: https://www.smart-soft.ru/blog/zaschita_informatsii_v_avtomatizirovannyh_sistemah (дата обращения: 11.06.2024).
2. Методы и средства разработки автоматизированных информационных систем на основе онтологии. URL: https://cyberleninka.ru/article/n/metody-i-sredstva-razrabotki-avtomatizirovannyh-informatsionnyh-sistem-na-osnove-ontologii-upravlenie-kachestvom-programmno/viewer (дата обращения: 15.06.2024).
3. Автоматизированные информационные системы и их возможности. URL: https://cyberleninka.ru/article/n/avtomatizirovannye-informatsionnye-sistemy-ais-i-ih-vozmozhnosti-ispolzovanie-programmy-ais-kachestvo-produktsii-na-predpriyatii/viewer (дата обращения: 21.06.2024).
4. Функциональная структура автоматизированной информационной системы профилактики безнадзорности и правонарушений. URL: https://cyberleninka.ru/article/n/funktsionalnaya-struktura-avtomatizirovannoy-informatsionnoy-sistemy-profilaktiki-beznadzornosti-i-pravonarusheniy/viewer (дата обращения: 11.07.2024).
5. Методы обеспечения информационной защиты. URL: https://domgadalki.ru/foto/metodiy-obespecheniya-informatsionnoy-zashitiy (дата обращения: 21.08.2024).
6. Концепция обеспечения безопасности информации. URL: https://res.sm-center.ru/sibir/File/6b3b75e5-03f9-4ae1-a11e-9bd850a7c513:Концепция.pdf (дата обращения: 11.09.2024).
7. Solodjannikov. Информационная безопасность. URL: https://infosec.spb.ru/wp-content/uploads/2020/08/solodjannikov.pdf (дата обращения: 15.09.2024).

8. Защита информации в автоматизированных системах. URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-informatsionnykh-sistemakh/v-avtomatizirovannykh-informatsionnykh-sistemakh/ (дата обращения: 18.09.2024).
9. 12 топовых IDS/IPS инструментов. URL: https://www.csoonline.com/article/569085/12-top-idsips-tools.html (дата обращения: 11.10.2024).
10. Selectel. Мониторинг информационной безопасности. URL: https://habr.com/ru/articles/790002/ (дата обращения: 11.10.2024).
11. Инструменты для управления идентификацией. URL: https://livebusiness.org/tools/identity_management/ (дата обращения: 11.10.2024)