УДК 004.056.5

Ю.С. Корякина, jk169@list.ru
Институт машиноведения, автоматики и геомеханики НАН КР
Институт информационных технологий КГТУ им. И.Раззакова
Нурбек уулу Сыймык, syiman.01@mail.ru
Институт информационных технологий КГТУ им. И.Раззакова
И.В. Зимин, igorzimin777@mail.ru
Академия цифровых инноваций

АНАЛИТИЧЕСКИЙ ОБЗОР ТЕХНОЛОГИЙ И МЕТОДОВ РАЗРАБОТКИ ПОДСИСТЕМЫ ЗАЩИТЫ СЕТЕВОГО ПЕРИМЕТРА ДЛЯ SOC

В данной статье были проанализированы современные методы защиты сетевого периметра для центра безопасности (SOC). Рассмотрены особенности и недостатки каждого подхода, а также области, в которых каждый метод является наиболее эффективным. Продемонстрированы зависимости уровня безопасности от внедрения различных технологий мониторинга и анализа трафика, а также показаны методы выявления и устранения киберугроз. Проанализировав существующие методы, автор рекомендует многоуровневую стратегию защиты сетевого периметра, обеспечивающую наиболее полное и достоверное выявление угроз. Подход, ориентированный на SOC, является наиболее эффективным по следующим причинам:

— централизованный сбор и корреляция событий безопасности;

— использование систем поведенческого анализа и машинного обучения;

— интеграция с SIEM для оперативного реагирования на инциденты;

— возможность автоматизированного устранения угроз;

— защита от сложных целевых атак за счёт постоянного обновления алгоритмов обнаружения.

Ключевые слова: SOC, Защита сетевого периметра, NGFW (следующее поколение файрвола), IDS/IPS, Threat Intelligence (TI), XDR (расширенное обнаружение и реагирование), AI/ML (искусственный интеллект / машинное обучение), Zero Trust Architecture (ZTA), SASE (безопасный доступ на основе облака), CASB (брокер безопасности облачного доступа), EDR (обнаружение и реагирование на конечных точках), MFA (многофакторная аутентификация), SIEM, NTA/NDR, TLS Inspection, Deception Technology, Microsegmentation, Security Awareness Training, Phishing Simulation, UEBA, IAM, DLP, SOAR автоматизация процессов SOC, виртуальные аналитики / AI-системы, Cyber Range / киберучебные полигоны.

Koryakin Sergey Vladimirovich srgkoryakin1@gmail.com
Institute of Mechanical Engineering, Automation and Geomechanics NAS KR
Institute of Information Technologies KSTU named after. I. Razzakova
Nurbek uulu Syimyk, syiman.01@mail.ru
Institute of Information Technologies KSTU named after. I. Razzakova
I.V. Zimin, igorzimin777@mail.ru
Academy of Digital Innovations

Введение

Современные центры мониторинга безопасности (SOC) играют ключевую роль в обеспечении защиты сетевого периметра организации. Развитие киберугроз требует

применения комплексных методов защиты, включающих как традиционные механизмы, так и передовые технологии на основе искусственного интеллекта и машинного обучения.

Актуальность темы исследования обусловлена ростом числа атак на сетевую инфраструктуру, усложнением методов взлома и необходимостью оперативного реагирования на инциденты безопасности.

Security Operations Center (SOC) играет ключевую роль в защите сетевого периметра, однако сталкивается с рядом проблем:

- **Высокий уровень ложных срабатываний** – большое количество алертов может затруднять выявление реальных угроз.
- **Недостаток квалифицированных специалистов** – нехватка экспертов в области кибербезопасности усложняет оперативное реагирование на инциденты.
- **Сложность интеграции разнородных систем** – необходимость синхронизации SIEM, IDS/IPS, Firewall и других систем.
- **Автоматизация процессов реагирования** – недостаток эффективных SOAR-решений может замедлять реакцию на атаки.
- **Обнаружение сложных угроз (APT)** – продвинутые постоянные угрозы могут оставаться незамеченными из-за их сложной структуры и маскировки[1,2].

Защита сетевого периметра представляет собой комплекс мер, направленных на предотвращение несанкционированного доступа к корпоративной сети, защиту от кибератак и обеспечение безопасности передаваемых данных. Современные угрозы требуют применения как технических, так и организационных решений для минимизации рисков. Основное разделение защиты сетевого периметра осуществляется на **внешнюю** и **внутреннюю** защиту.

Внешняя защита сетевого периметра. Целью внешней защиты является предотвращение атак и несанкционированного доступа из внешней сети (например, из Интернета). Для этого применяются следующие методы и технологии:

- **Межсетевые экраны (Firewall).** Контролируют и фильтруют входящий и исходящий трафик на основе заданных правил. Различают следующие типы:
  – Пакетные фильтры, анализируют заголовки пакетов и пропускают или блокируют их в зависимости от настроек.
  – Stateful Firewall, отслеживает состояния соединений и блокирует подозрительный трафик.
  – Приложенческий Firewall (WAF) защищает веб-приложения от атак, таких как SQL-инъекции и XSS.
- **Системы предотвращения и обнаружения вторжений (IDS/IPS)** – **с**истемы обнаружения вторжений, анализирующие трафик на предмет подозрительной активности.
- **IPS (Intrusion Prevention System)** – системы предотвращения вторжений, которые не только выявляют атаки, но и могут автоматически блокировать их.
- **Виртуальные частные сети (VPN).** Используется для безопасного соединения удалённых пользователей и филиалов с внутренней сетью организации. Применяются протоколы **IPSec, SSL/TLS и WireGuard** для шифрования передаваемых данных.
- **Анти-DDoS решения.** DDoS-атаки могут нарушить работу инфраструктуры организации.

  Для защиты применяются:

- Облачные анти-DDoS сервисы.
- Аппаратные и программные решения для фильтрации трафика
- Rate-limiting и blackhole routing для блокировки вредоносных запросов.

- **Демилитаризованная зона (DMZ).** DMZ – это сегмент сети, предназначенный для размещения публичных ресурсов (веб-серверов, почтовых серверов, DNS). Внешние пользователи могут обращаться к этим ресурсам без доступа к внутренней сети.
- **Внутренняя защита сетевого периметра.** Считается, что внутренние угрозы включают следующие направления – компрометация учетных записей, заражение рабочих станций, атаки инсайдеров [3,4].

  Для защиты применяются следующие технологии:

- **Контроль доступа (NAC)**

Network Access Control (NAC) позволяет проверять устройства перед их подключением к сети. Если устройство не соответствует требованиям безопасности (отсутствуют обновления, антивирус и т. д.), его доступ ограничивается.

- **Сегментация сети**

  Разделение сети на изолированные сегменты с использованием VLAN или Zero Trust модели позволяет ограничить движение вредоносного кода и минимизировать возможный ущерб от атаки.
- **Мониторинг и анализ событий безопасности (SIEM)**

  Системы управления событиями безопасности (SIEM) собирают и анализируют журналы событий, выявляют аномалии и позволяют оперативно реагировать на инциденты.
- **Контроль привилегированных пользователей (PAM)**

  Применение решений Privileged Access Management (PAM) ограничивает права доступа администраторов, предотвращая несанкционированное изменение критически важных системных параметров.
- **Защита от внутренних угроз (DLP)**

  Data Loss Prevention (DLP) контролирует перемещение конфиденциальных данных и предотвращает их утечку через e-mail, мессенджеры, USB-накопители[5,6].

Антивирусная защита и EDR

- **Антивирусные системы** выявляют и блокируют вредоносные программы.
- **EDR (Endpoint Detection and Response)** отслеживает аномальную активность на рабочих станциях и серверах, предотвращая угрозы.

С увеличением числа кибератак, сложностью методов взлома и постоянным развитием технологий киберпреступников защита сетевого периметра становится критически важной задачей. Традиционные методы уже не способны полностью нейтрализовать современные угрозы, такие как атаки с применением машинного обучения или сложные многоступенчатые вторжения. В связи с этим требуется интеграция новых подходов, автоматизированных систем анализа угроз и проактивных стратегий защиты[7,8].

Основные угрозы сетевого периметра SOC. Перед разработкой методов защиты необходимо учитывать основные угрозы, такие как (табл.1):

Таблица 1 – Угрозы и описание

Угроза	Описание
DDoS-атаки	Перегрузка сети ложными запросами
Эксплуатация уязвимостей	Использование недостатков ПО и оборудования
Фишинг	Социальная инженерия для получения данных
Вредоносное ПО	Внедрение вредоносных программ
Несанкционированный доступ	Взлом аккаунтов и систем
Ботнет-атаки	Использование зараженных устройств
Атаки на цепочки поставок	Компрометация поставщиков ПО и оборудования

Методы защиты сетевого периметра. Для эффективной защиты сетевого периметра SOC используются различные подходы, которые можно разделить на традиционные и современные технологии.

Традиционные методы защиты:

- ✓ Межсетевые экраны (Firewall) – фильтрация трафика на основе правил;
- ✓ Системы обнаружения и предотвращения вторжений (IDS/IPS);
- ✓ Виртуальные частные сети (VPN) для защиты удаленного доступа;
- ✓ Сегментация сети для минимизации последствий атак;
- ✓ Антивирусные решения и защита от вредоносного ПО.

Современные технологии и подходы защиты сетевого периметра (табл.2):

Таблица 2 – Технологии и описании

Технология	Описание
Анализ трафика на основе машинного обучения	Обнаружение аномалий и угроз
Zero Trust Architecture (ZTA)	Проверка каждого запроса независимо от его происхождения
Security Information and Event Management (SIEM)	Мониторинг и корреляция событий безопасности
Deception-технологии	Создание ловушек для атакующих
Автоматизация SOC (SOAR)	Автоматизированное реагирование на инциденты
UEBA	Анализ аномалий поведения пользователей

Инструменты и платформы защиты. Для защиты сетевого периметра SOC применяются следующие инструменты:

- ✓ SIEM-системы (Splunk, IBM QRadar, ArcSight);
- ✓ IDS/IPS- решения (Snort, Suricata, Zeek);
- ✓ NGFW (Palo Alto Networks, Cisco Firepower);
- ✓ DDoS-защита (Cloudflare, Akamai, Radware);
- ✓ Средства анализа поведения пользователей (UEBA – User and Entity Behavior Analytics);
- ✓ Облачные платформы безопасности (Microsoft Defender, Google Chronicle).

Сравнение моделей защиты. Для определения наиболее эффективных методов защиты проведено сравнение нескольких подходов, ниже приведена таблица с технологиями, методами и способами решения для защиты сетевого периметра SOC, с более детальным описанием[9,10] (табл.3).

Таблица 3 – Существующие технологии и методы

Технологии и методы	Описание	Применение/Решения
Next-Generation Firewall (NGFW)	Фильтрация трафика на уровне приложений, контроль за использованием приложений и пользователей	Защита от внешних атак, блокировка нежелательного трафика, фильтрация приложений и контента
Intrusion Detection/Prevention Systems (IDS/IPS)	Системы обнаружения и предотвращения вторжений, анализ сетевого трафика для выявления атак	Обнаружение и блокировка сетевых атак, анализ и корреляция событий
Threat Intelligence (TI)	Использование информации о новых угрозах и уязвимостях для защиты от атак	Интеграция с SIEM, повышение оперативности реагирования, блокировка атак на основе известных индикаторов угроз
XDR (Extended Detection and Response)	Расширенное обнаружение и реагирование на угрозы, объединяющие данные из различных источников	Комплексная защита на уровне всех систем (конечные устройства, сеть, серверы) с централизованным анализом угроз
AI/ML для анализа аномалий	Использование искусственного интеллекта для анализа сетевого трафика и поведения пользователей	Автоматическое выявление подозрительных паттернов, снижение нагрузки на аналитиков
Zero Trust Architecture (ZTA)	Архитектура, при которой ни одно устройство или пользователь не имеет доверия, каждый запрос проверяется	Ужесточение контроля доступа, минимизация рисков от внутренних и внешних угроз
Secure Access Service Edge (SASE)	Объединение защиты сети и облачных сервисов в одной платформе	Защита удалённых пользователей и облачных сервисов, упрощение управления безопасностью
Cloud Access Security Broker (CASB)	Средства контроля доступа и мониторинга облачных приложений	Защита данных и контроль за доступом в облачные сервисы
Endpoint Detection and Response (EDR)	Защита и мониторинг конечных устройств с фокусом на безопасность рабочих станций и серверов	Реагирование на инциденты, мониторинг поведения на устройствах, защита от атак на конечных точках
Многофакторная аутентификация (MFA)	Требование более чем одного метода аутентификации для входа в систему	Повышение безопасности доступа, защита учетных записей от компрометации
SIEM (Security Information and Event Management)	Система для сбора, хранения и анализа логов и событий безопасности	Централизованный сбор данных безопасности, корреляция инцидентов, аналитика угроз
Network Traffic Analysis (NTA)	Анализ сетевого трафика с целью выявления аномальных или подозрительных активностей	Выявление угроз в реальном времени, предотвращение атак до их реализации
TLS Inspection	Инспекция зашифрованного трафика для выявления скрытых угроз	Повышение видимости в зашифрованном трафике, защита от атак, скрывающихся за шифрованием
Deception Technology	Создание ложных целей для атакующих, чтобы запутать их и собрать информацию	Привлечение внимания атакующих к ложным целям, улучшение выявления и анализа угроз
Microsegmentation	Разделение сети на маленькие сегменты с индивидуальными правилами безопасности для каждого	Снижение возможности распространения атак внутри сети, контроль доступа между сегментами
Security Awareness Training	Программы обучения сотрудников для повышения осведомленности о безопасности	Обучение сотрудников безопасному поведению в сети, предотвращение фишинга и других атак
Phishing Simulation	Симуляция фишинговых атак для тестирования сотрудников на устойчивость	Проверка сотрудников на осведомленность о фишинге, тренировка их на выявление фальшивых сообщений
UEBA (User and Entity Behavior Analytics)	Анализ поведения пользователей и устройств для выявления аномальной активности	Выявление инсайдерских угроз, подозрительного поведения, попыток доступа к критической информации
IAM (Identity and Access Management)	Управление доступом к корпоративным ресурсам на основе идентификации пользователей	Контроль прав доступа, предотвращение несанкционированного доступа, внедрение политики минимальных привилегий
DLP (Data Loss Prevention)	Технологии защиты от утечек данных и нежелательного распространения информации.	Защита конфиденциальных данных, предотвращение их утечки или несанкционированного использования
SOAR (Security Orchestration, Automation, and Response)	Автоматизация процессов реагирования на инциденты и управление операциями безопасности	Снижение времени реакции на инциденты, улучшение координации действий между системами и людьми
AI/ML в кибербезопасности	Использование машинного обучения и	Автоматическое обнаружение новых атак,

	искусственного интеллекта для автоматического анализа и реагирования на угрозы	корреляция событий и предсказание атак
Автоматизированный анализ логов	Использование алгоритмов для быстрого анализа логов безопасности	Снижение нагрузки на аналитиков, быстрая идентификация инцидентов
Cyber Range	Виртуальные тренировочные площадки для киберспециалистов, где моделируются реальные угрозы	Обучение специалистов, подготовка к реальным инцидентам, тестирование реакций SOC
Bug Bounty программы	Программы, в которых исследователи безопасности находят уязвимости и сообщают о них за вознаграждение	Привлечение внешних специалистов для поиска уязвимостей, повышение безопасности продуктов
Аутсорсинг SOC (MSSP)	Внешние компании, которые предоставляют услуги мониторинга и защит	Снижение затрат на создание собственного SOC, использование опыта внешних специалистов

Ниже представлена таблица с преимуществами и недостатками технологий и методов для защиты сетевого периметра SOC (табл.4):

Таблица 4 – Преимущества и недостатки существующих технологий и методов

Проблема	**Решение (технологии, методы)**	**Преимущества**	**Недостатки**
1□. Рост количества и сложности кибератак	**NGFW (Next-Generation Firewall)**	Глубокий анализ трафика, контроль на уровне приложений, предотвращение атак	Высокая стоимость, требует грамотной настройки
	IDS/IPS (Intrusion Detection/Prevention Systems)	Выявление и блокировка атак, анализ сетевого трафика	Возможны ложные срабатывания, сложная настройка
	Threat Intelligence (TI)	Обнаружение актуальных угроз, повышение эффективности SOC	Требует интеграции с SIEM, не предотвращает атаки, а только информирует
	XDR (Extended Detection and Response)	Корреляция данных из разных источников, улучшенное обнаружение атак	Требует сложной настройки и интеграции
	AI/ML для анализа аномалий	Автоматическое выявление угроз, снижение нагрузки на аналитиков	Может давать ложные срабатывания, требует обученных моделей
2□. Уязвимость удалённой работы и облачных сервисов	**Zero Trust Architecture (ZTA)**	Минимизация риска атак, строгий контроль доступа	Требует кардинального пересмотра ИТ-инфраструктуры
	SASE (Secure Access Service Edge)	Интеграция сетевой безопасности и защиты облачных сервисов	Сложная реализация, высокая стоимость
	CASB (Cloud Access Security Broker)	Мониторинг облачных сервисов, контроль доступа	Возможны сложности интеграции с существующими сервисами
	EDR (Endpoint Detection and Response)	Защита конечных устройств, анализ аномалий	Требует мощных вычислительных ресурсов
	MFA (Многофакторная аутентификация)	Повышенная защита учетных записей	Усложняет доступ для пользователей
3□. Отсутствие полной видимости и контроля за трафиком	**SIEM (Security Information and Event Management)**	Централизованный анализ логов, корреляция событий	Высокая стоимость, сложность настройки
	NTA/NDR (Network Traffic Analysis / Network Detection and Response)	Глубокий анализ сетевого трафика, обнаружение скрытых атак	Требует мощных ресурсов, может вызывать задержки
	TLS Inspection	Анализ зашифрованного трафика, выявление вредоносных действий	Высокая нагрузка на оборудование, вопросы конфиденциальности
	Deception Technology	Ловушки для атакующих, защита от внутренних угроз	Сложность внедрения, возможны ложные срабатывания
	Microsegmentation	Контроль передвижения данных в сети, снижение риска распространения угроз	Требует модернизации инфраструктуры
4□. Высокая зависимость от человеческого фактора	**Security Awareness Training**	Снижение вероятности фишинга, повышение уровня знаний сотрудников	Требует регулярного обучения, не защищает от сложных атак
	Phishing Simulation	Проверка сотрудников на устойчивость к фишингу	Может вызывать негативную реакцию сотрудников
	UEBA (User and Entity Behavior Analytics)	Анализ поведения пользователей, выявление подозрительной активности	Требует больших данных и вычислительных мощностей
	IAM (Identity and Access Management)	Управление доступом, предотвращение компрометации учетных записей	Сложность внедрения, возможны ошибки конфигурации
	DLP (Data Loss Prevention)	Защита от утечек данных	Может мешать рабочим процессам, требует точной

			настройки
5□. Недостаточная автоматизация процессов SOC	**SOAR (Security Orchestration, Automation, and Response)**	Автоматизация обработки инцидентов, снижение нагрузки на аналитиков	Высокая стоимость внедрения, требует интеграции с SOC
	Автоматизированные Playbooks	Быстрое реагирование на угрозы, снижение человеческого фактора	Ограниченная гибкость, требует постоянного обновления
	AI/ML в кибербезопасности	Анализ и выявление угроз в реальном времени	Возможны ложные срабатывания, требует постоянного обучения
	Автоматизированный анализ логов	Уменьшение нагрузки на аналитиков SOC	Требует SIEM или других аналитических платформ
	Автоматизация рутинных задач (SOAR, AI-аналитика)	Снижение нагрузки на аналитиков, ускорение реагирования	Не заменяет полностью специалистов, требует поддержки
	Виртуальные аналитики (AI-системы)	Помощь в анализе инцидентов, повышение эффективности SOC	Требует значительных инвестиций, не заменяет человека
	Cyber Range (киберучебные полигоны)	Подготовка кадров, повышение квалификации сотрудников	Высокая стоимость создания и поддержки
	Bug Bounty программы	Поиск уязвимостей, привлечение внешних экспертов	Возможны риски утечек, требует грамотного управления
6□. Нехватка квалифицированных специалистов	**Аутсорсинг SOC (MSSP, Managed Security Service Providers)**	Экономия на найме сотрудников, круглосуточный мониторинг	Потеря контроля над процессами, возможные задержки в реагировании

В ходе исследования и анализа различных решений для защиты сетевого периметра были рассмотрены несколько ведущих технологий: NGFW, NDR, SOAR, SIEM и Threat Intelligence-платформы. Основной целью было выявить оптимальное сочетание инструментов, обеспечивающее глубокую защиту сети с автоматизацией процессов реагирования на инциденты[11,12].

После анализа стало очевидно, что **ни одно отдельное решение не охватывает все аспекты защиты**, поэтому наиболее эффективным является **комбинированный подход (рис.1)**.

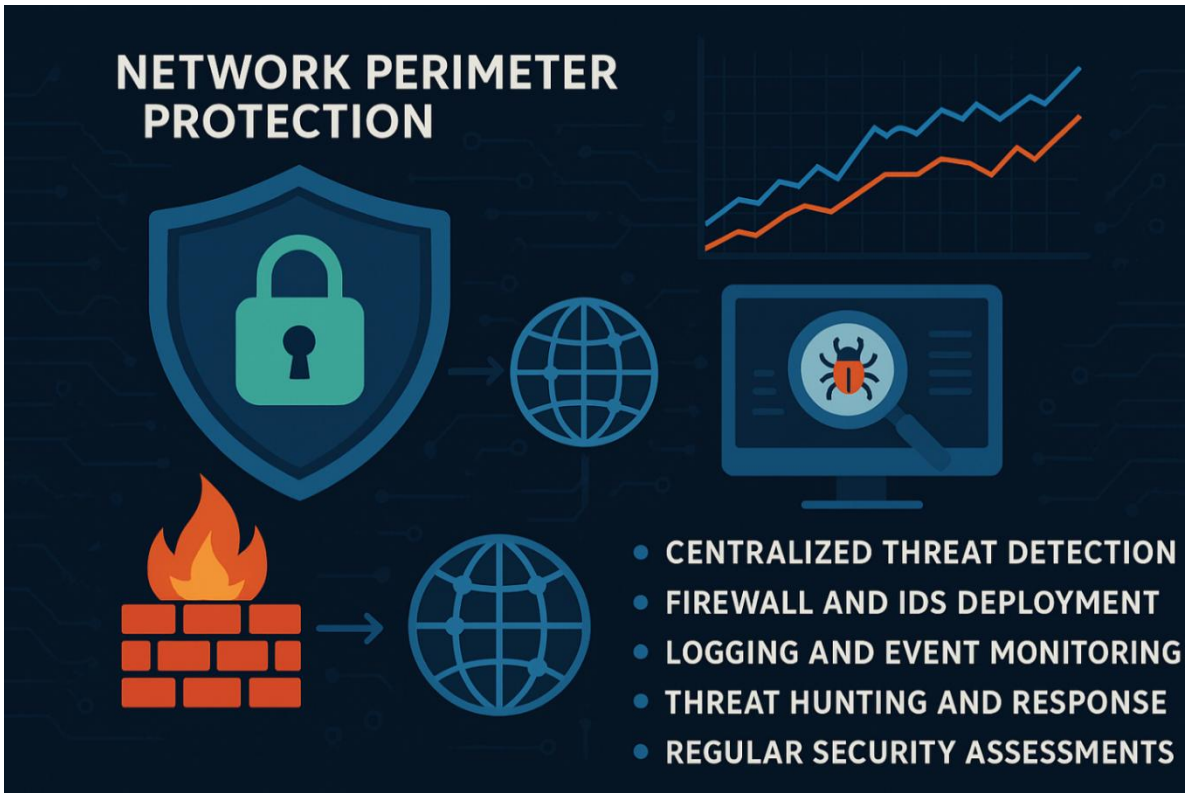

Рисунок 1 – Совместное использование инструментов NGFW, NDR, SOAR, SIEM и Threat Intelligence

Следует отметить, что совместное использование инструментов, указанных на рисунке 1, обуславливается следующими техническими характеристиками:

Palo Alto NGFW + Cisco Secure Firewall & Umbrella – мощная защита **на границе сети**, контроль трафика, фильтрация и предотвращение атак.

Darktrace NDR – **AI-анализ** сетевых аномалий и скрытых угроз внутри сети.

XSOAR (SOAR) – **автоматизированное реагирование**, интеграция с SIEM, фаерволами и TI-платформами.

Cisco Talos + Palo Alto WildFire + STIX/TAXII – мощная система **Threat Intelligence** для предиктивной защиты.

Преимущества этого выбора:

1. *Комплексный подход:* охватывает **внешние и внутренние угрозы**.
2. *Автоматизация реагирования*: сокращает время реакции на инциденты.
3. *Гибкость**:*** работает в **локальных, облачных и гибридных** средах
4. *Лучшие технологии в своих классах**: лидеры*** рынка в каждом сегменте.

Преимущества каждого компонента:

– **Palo Alto NGFW**, защита периметра с функцией анализа трафика на уровне приложений (L7).

– **Cisco Secure Firewall & Umbrella** – фильтрация трафика, защита DNS, VPN и Zero Trust Access.

– **Darktrace NDR (Network Detection & Response)** – AI-анализ аномалий внутри сети.

– **XSOAR (Palo Alto Cortex XSOAR)** – автоматизация реагирования, интеграция SOC[13].

Рассмотрим характеристики решений, использующиеся на границе сети (между Интернетом и корпоративной сетью):

1. Palo Alto NGFW — защита периметра сети

Функции:

-Анализ трафика на уровне **L7 (Deep Packet Inspection).**

-Фильтрация трафика: **URL Filtering, SSL Decryption.**

-IPS/IDS – предотвращение атак и вторжений.

-WildFire (Threat Intelligence) – анализ вредоносных файлов.

-Защита от **Zero-Day атак.**

2. Cisco Secure (NGFW + Umbrella) — расширенная защита сети, используемая на границе сети + защита удалённых пользователей.

Функции:

-Фильтрация трафика на **межсетевом экране** (NGFW).

-Cisco Umbrella – защита на уровне **DNS (Secure Web Gateway).**

-VPN и Zero Trust – безопасный удалённый доступ.

-Интеграция с **Cisco Talos** для Threat Intelligence.

3. Darktrace NDR — обнаружение угроз внутри сети

Функции:

-AI-анализ аномалий (поведенческий анализ трафика).

-Выявление **внутренних угроз** (Insider Threats).

-Детектирование атак **Command & Control (C2).**

-Обнаружение **медленных атак (Low & Slow).**

4. XSOAR (Palo Alto Cortex XSOAR) — автоматизация SOC (SOAR)

Функции:

-**Автоматическое реагирование** на инциденты.

-Интеграция с **SIEM, NGFW, NDR, EDR.**

-**Оркестрация безопасности** – управление процессами SOC.

-Threat Intelligence: поддержка **STIX/TAXII, IBM X-Force, Cisco Talos.**

Нормативное регулирование и стандарты. Считается, что для обеспечения соответствия требованиям безопасности используются следующие стандарты (табл.5):

Таблица 5 – Соответствие стандартам

Стандарт	Описание
ISO/IEC 27001	Управление информационной безопасностью
NIST Cybersecurity Framework	Рекомендации по управлению рисками
GDPR	Регламент защиты данных в Европе
FISMA	Закон о безопасности критической инфраструктуры (США)
ENISA	Директивы по кибербезопасности в ЕС

Примеры реализации и лучшие практики: Компании, такие как Google, Microsoft и Amazon, применяют комплексные подходы к защите сетевого периметра, включая Zero Trust, автоматизированный анализ угроз и интеграцию SIEM/SOAR.

Лучшие практики обеспечения безопасности SOC[14]:

- Принцип минимальных привилегий – ограничение доступа к ресурсам по необходимости.
- Регулярный аудит безопасности – оценка состояния инфраструктуры и поиск уязвимостей.
- Многофакторная аутентификация (MFA) – защита учетных записей от компрометации.
- Мониторинг и корреляция событий – автоматизированный анализ активности пользователей.
- Резервное копирование и восстановление – регулярное создание резервных копий для предотвращения потери данных.
- Тестирование на проникновение (Pentesting) – проверка системы на устойчивость к атакам.
- Обучение сотрудников – повышение осведомленности персонала о киберугрозах.
- Использование threat intelligence – анализ актуальных угроз и упреждающее реагирование.

Подводя итоги, следует отметить, что обеспечение защиты сетевого периметра в рамках Центра обеспечения безопасности (SOC) представляет собой многослойную и комплексную задачу, требующую интеграции классических подходов, современных технологических решений и высокоавтоматизированных процессов. Эффективность данной системы в значительной степени определяется способностью своевременно адаптироваться к динамично изменяющемуся ландшафту киберугроз и инновационному развитию средств нападения. В условиях устойчивого роста числа и сложности кибератак особую актуальность приобретает необходимость стратегических инвестиций в перспективные технологии кибербезопасности, повышение уровня квалификации специалистов, а также внедрение проверенных практик и стандартов информационной безопасности.

Список использованных источников

1. Аксенов К.Ю. Информационная безопасность: защита сетей и систем // М.: Инфра-М, 2020. – 352 с.
2. Бойко А.Ю., Костин И.А. Технологии защиты периметра корпоративной сети: учебное пособие. – СПб.: Питер, 2021. – 288 с.
3. Принципы построения центров мониторинга информационной безопасности (SOC). – М.: РОСИНФОРМТЕХ, 2019. – 212 с.
4. Беляев В.И. Сетевые технологии и защита информации: монография. – М.: Академия, 2020. – 416 с.
5. Гиляров А.В., Зайцев Д.А. Методы обнаружения атак в системах мониторинга безопасности // Вестник компьютерных и информационных технологий. – 2022. – №2. – С. 55–63.
6. Нестеренко Л.А., Калмыков А.С. Анализ угроз информационной безопасности в корпоративных сетях // Информационные технологии. – 2021. – №9. – С. 22–28.
7. ISO/IEC 27001:2022. Information technology – Security techniques – Information security management systems – Requirements. – Geneva: ISO, 2022.
8. Национальный стандарт Российской Федерации. ГОСТ Р 57580.1–2017. Защита информации. Безопасность финансовых организаций. Общие требования. – М.: Стандартинформ, 2018.
9. Stallings W. Network Security Essentials: Applications and Standards. – 6th ed. – Boston: Pearson Education, 2022. – 480 p.
10. Scarfone K., Mell P. Guide to Intrusion Detection and Prevention Systems (IDPS). – NIST Special Publication 800-94. – Gaithersburg: NIST, 2007.
11. Anton A., Killcrece G. Building a Security Operations Center: A Strategic Guide. – SANS Institute, 2019. – 87 p.
12. Лебедев С.Н., Мишустин И.В. Методология построения SOC: современное состояние и перспективы // Информационные технологии и безопасность. – 2023. – Т. 12, №4. – С. 41–49.
13. Cisco Systems. Cisco Security Architecture for the Enterprise. – Cisco White Paper, 2021. – URL: https://www.cisco.com (дата обращения: 10.06.2025).
14. Palo Alto Networks. The SOC Transformation Model. – Palo Alto White Paper, 2022. – URL: https://www.paloaltonetworks.com (дата обращения: 10.06.2025).