

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ  
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ  
«БРЕСТСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ  
УНИВЕРСИТЕТ»  
ФАКУЛЬТЕТ ЭЛЕКТРОННО-ИНФОРМАЦИОННЫХ СИСТЕМ  
Кафедра интеллектуальных информационных технологий

**РЕФЕРАТ**  
по дисциплине  
«Современные методы защиты компьютерных систем»

Выполнил:  
Студент 4 курса  
ФЭИС  
группы ИИ-22  
Сидоренко А.А.

Брест 2024

## 1 SOC

В условиях современной цифровизации и глобальной сетевой взаимосвязанности, вопросы безопасности данных и информационных систем становятся всё более актуальными. Одним из ключевых элементов обеспечения безопасности является создание и эффективное функционирование **Центра Операций Безопасности (SOC, от англ. Security Operations Center)**. SOC представляет собой специализированное подразделение, предназначенное для мониторинга, анализа и реагирования на угрозы безопасности, с целью защиты информационных систем и данных организации от атак и инцидентов. **SOC (Security Operations Center)** — это центр, обеспечивающий круглосуточный мониторинг, анализ и управление событиями информационной безопасности. Главная цель SOC заключается в обнаружении, предотвращении и реагировании на кибератаки и инциденты безопасности, а также в обеспечении защиты информационных активов организации. SOC может быть как внутренним подразделением компании, так и внешней службой, предоставляющей услуги по аутсорсингу. SOC выполняет несколько важнейших функций, которые включают:

**Мониторинг и анализ угроз:** SOC занимается непрерывным мониторингом трафика, сетевых активностей, журналов событий и систем для выявления аномальных или подозрительных действий, которые могут указывать на потенциальную угрозу.

**Обнаружение инцидентов безопасности:** Основная задача SOC — своевременно выявлять инциденты безопасности, такие как кибератаки, вторжения, вредоносное ПО, утечки данных и другие угрозы.

**Реагирование на инциденты:** В случае обнаружения угрозы SOC принимает меры по нейтрализации инцидента. Это может включать блокировку вредоносного трафика, изоляцию заражённой системы, устранение уязвимостей или восстановление после атаки.

**Управление уязвимостями:** SOC оценивает уязвимости информационных систем и помогает устранять их до того, как они будут использованы злоумышленниками.

**Соблюдение нормативных требований:** SOC помогает организации соответствовать стандартам безопасности и соблюдения законодательства, таким как GDPR, PCI DSS, ISO

27001 и другие, путем мониторинга и отчетности. **Анализ угроз и угрозы снаружи:** SOC анализирует потенциальные угрозы и уязвимости в глобальной сети, отслеживает новые методы атак, чтобы заранее подготовиться к их возможному применению. Для эффективной работы SOC использует ряд технологий, которые помогают в мониторинге и реагировании на инциденты безопасности:

- **SIEM (Security Information and Event Management):** Это системы, которые собирают, нормализуют и анализируют данные о событиях из различных источников (системы, сети, устройства безопасности и т. д.), чтобы выявить возможные угрозы.
- **IDS/IPS (Intrusion Detection/Prevention Systems):** Системы обнаружения и предотвращения вторжений, которые позволяют автоматически реагировать на угрозы в реальном времени.
- **SOAR (Security Orchestration, Automation and Response):** Платформы для автоматизации процессов реагирования на инциденты и интеграции различных инструментов безопасности в единую систему.
- **Threat Intelligence Platforms:** Платформы для сбора и анализа информации о текущих угрозах и уязвимостях, которая помогает организациям заранее готовиться к возможным атакам.
- **EDR (Endpoint Detection and Response):** Решения для мониторинга конечных устройств и быстрого реагирования на угрозы, исходящие от них.

## **2 FW/NGFW**

В современных условиях киберугроз и расширяющихся возможностей атакующих, защита информационных систем и сетевой инфраструктуры становится одной из важнейших задач для организаций любого уровня. Одним из ключевых компонентов системы безопасности является использование межсетевых экранов (firewall). В последние годы на смену традиционным межсетевым экранам приходят новые решения, которые обеспечивают более высокий уровень защиты. Это так называемые следующие поколения межсетевых экранов (Next-Generation Firewall, NGFW). В данном реферате будут рассмотрены основные характеристики, различия и преимущества традиционных межсетевых экранов (FW) и NGFW.

### **Традиционные межсетевые экраны (FW)**

Межсетевой экран (Firewall, FW) — это система безопасности, предназначенная для фильтрации входящего и исходящего сетевого трафика в зависимости от заранее установленных правил. Принцип работы традиционного межсетевого экрана заключается в том, чтобы блокировать нежелательный трафик, исходя из анализа определенных характеристик, таких как:

- **IP-адреса** источников и получателей.
- **Порты** и протоколы (TCP, UDP и др.).
- **Типы пакетов** (например, на основе анализа заголовков).

Традиционные межсетевые экраны обычно действуют на уровне сетевого или транспортного слоя модели OSI и осуществляют лишь базовую фильтрацию трафика, ограничиваясь проверкой информации о подключении и простыми правилами.

### **Межсетевые экраны нового поколения (NGFW)**

Next-Generation Firewall (NGFW) — это более современное решение, которое объединяет традиционные функции межсетевых экранов с новыми возможностями для защиты от более сложных угроз. NGFW предлагают расширенную функциональность, которая включает в себя не только фильтрацию на уровне сетевого трафика, но и: **Глубокий анализ пакетов (DPI, Deep Packet**

**Inspection).** NGFW анализируют содержимое пакетов, что позволяет обнаруживать угрозы на уровне приложений, например, вирусы, шпионские программы и другие формы вредоносного кода. **Интеграция с системами предотвращения вторжений (IPS).** Эти системы могут предотвращать атаки и блокировать подозрительную активность, реагируя на определенные паттерны поведения. **Контроль приложений.** NGFW позволяют фильтровать трафик по приложениям, а не только по порту или IP-адресу. Например, блокировка доступа к социальным сетям или мессенджерам. **Антивирусная защита.** Встроенные механизмы антивирусной фильтрации помогают выявлять и блокировать вредоносные файлы, даже если они зашифрованы. **Шифрование трафика.** NGFW способны анализировать зашифрованный трафик, что делает невозможным использование SSL/TLS туннелей для обхода фильтрации. **Контроль пользователей и устройств.** Некоторые решения NGFW позволяют интегрировать механизмы аутентификации и идентификации пользователей, а также контролировать подключенные устройства.

### Сравнение FW и NGFW

Характеристика	FW	NGFW
<b>Функциональность</b>	Базовая фильтрация трафика	Глубокая фильтрация, анализ на уровне приложений
<b>Уровень анализа</b>	Только заголовки пакетов	Заголовки пакетов + содержимое пакетов (DPI)
<b>Защита от атак</b>	Защита от атак на уровне сети	Защита от атак на уровне приложений, шифрование, IPS
<b>Механизмы предотвращения</b>	Отсутствуют или ограничены	Системы предотвращения вторжений, антивирусные технологии

<b>Характеристика</b>	<b>FW</b>	<b>NGFW</b>
<b>Сложность настройки</b>	Простота и минимальные настройки	Более сложная настройка и управление
<b>Стоимость</b>	Низкая	Высокая

### **Применение FW и NGFW**

Традиционные межсетевые экраны (FW) остаются актуальными для небольших сетевых инфраструктур, где необходимо только базовое разделение трафика между внутренними и внешними сегментами сети, а также защита от простых угроз. Они также могут использоваться в небольших офисах, где требования безопасности не столь высоки. NGFW, в свою очередь, более эффективно применяются в крупных и средних организациях, где необходима защита от более сложных и многогранных угроз, таких как атаки на веб-приложения, шифрование трафика, вирусы и другие формы зловредного ПО. NGFW также активно используются в облачных сервисах и в организации гибридных инфраструктур, где требуется защита как от внутренних угроз, так и от внешних атак.

### 3 IDS/IPS

IDS (Intrusion Detection System) и IPS (Intrusion Prevention System) — это два ключевых компонента современной системы безопасности информационных технологий, предназначенные для защиты сетей и серверов от различных видов атак и угроз. IDS и IPS выполняют схожие функции, однако их назначение и способы работы имеют определённые различия. IDS в первую очередь служит для обнаружения вторжений, а IPS помимо обнаружения также активно предотвращает или блокирует атаки. В данном реферате рассмотрены основные принципы работы, различия, преимущества и недостатки этих систем, а также их роль в обеспечении безопасности сети.

**IDS (Intrusion Detection System)** — система обнаружения вторжений. Она предназначена для мониторинга трафика сети, анализа данных и выявления аномалий, которые могут свидетельствовать о попытке вторжения или атаки. Основной задачей IDS является уведомление администратора о возможных угрозах, но она не блокирует эти угрозы автоматически.

**IPS (Intrusion Prevention System)** — система предотвращения вторжений. В отличие от IDS, которая лишь информирует о проблемах, IPS может не только обнаруживать атаки, но и принимать меры по их блокированию в реальном времени. IPS интегрируются с сетевой инфраструктурой, принимая активное участие в управлении трафиком и предотвращении вторжений.

#### Принцип работы IDS

Система IDS работает по одному из следующих принципов. **Сигнатурный анализ** — метод, основанный на сравнении сетевого трафика с заранее известными "подписями" атак. Это позволяет быстро обнаружить известные угрозы. Однако такой подход не эффективен для защиты от новых, ещё не идентифицированных атак. **Аномалистический анализ** — система анализирует нормальные шаблоны поведения в сети и сигнализирует о любых отклонениях от этих норм. Это позволяет выявить новые, неизвестные атаки, но может привести к ложным срабатываниям. **Гибридный подход** — комбинированный метод, использующий как сигнатурный, так и аномалистический анализ. Это

повышает точность обнаружения угроз и снижает количество ложных срабатываний.

### **Принцип работы IPS**

IPS работает на основе схожих методов, но в отличие от IDS, она выполняет не только анализ, но и действия, направленные на предотвращение атак.

**Сигнатурный подход** — IPS может блокировать трафик, который соответствует известным шаблонам атак. **Аномалистический анализ** — если система

обнаруживает аномалии в трафике, она может принять решение о блокировке подозрительных соединений или о маршрутизации трафика через

дополнительные фильтры для более глубокого анализа. **Реализация правил в**

**реальном времени** — IPS, интегрированная в сеть, принимает решения на основе текущей ситуации, автоматически блокируя попытки вторжения.

Системы IDS и IPS становятся важными компонентами в стратегиях киберзащиты. Они активно используются для защиты корпоративных сетей, облачных сервисов и других инфраструктурных объектов. Современные решения часто интегрируют функции IDS и IPS в одну систему, создавая более эффективные и гибкие средства защиты.



## 4 NTA

National Testing Agency (NTA) — это автономная организация, которая была основана правительством Индии в 2017 году с целью проведения различных национальных экзаменов и оценки квалификации кандидатов. Ее основная задача заключается в разработке, организации и администрировании экзаменов для студентов, аспирантов и профессионалов, что обеспечивает справедливость и прозрачность в процессе оценки знаний и навыков. NTA была создана с целью улучшения процесса экзаменов в Индии и устранения недостатков в существующих системах. До ее создания экзамены для студентов и кандидатов на различные образовательные и профессиональные программы проводились различными государственными и частными органами, что приводило к несоответствиям в качестве и организации. Создание NTA было обусловлено необходимостью единого стандарта для проведения экзаменов, увеличения числа доступных мест для экзаменов, повышения качества оценки и снижения стресса у кандидатов. Правительство Индии поручило NTA проводить такие важные экзамены, как JEE (Joint Entrance Examination), NEET (National Eligibility cum Entrance Test) и другие.

### Основные функции и задачи NTA

- **Разработка и проведение экзаменов:** Организация и проведение экзаменов для поступления в учебные заведения на разные уровни образования — от бакалавриата до аспирантуры.
- **Публикация результатов:** После завершения экзаменов NTA обеспечивает публикацию результатов и проводит анализ качества оценки.
- **Сертификация и лицензирование:** Организация сертификационных экзаменов для профессиональных квалификаций в различных областях.
- **Обеспечение прозрачности и честности:** Система электронных протоколов и строгие меры безопасности, такие как биометрия и электронные носители, помогают исключить возможность мошенничества и фальсификаций.

NTA проводит множество крупных национальных экзаменов, среди которых наиболее известные. **JEE Main:** Экзамен для поступления в инженерные учебные заведения, такие как ИТ (Indian Institutes of Technology) и НИТ (National Institutes of Technology). Экзамен проводится дважды в год и является важным этапом для студентов, стремящихся получить степень бакалавра в области инженерии. **NEET:** Национальный экзамен, проводимый для поступления в медицинские и стоматологические колледжи. NEET является обязательным для всех кандидатов, желающих учиться в медицинских вузах Индии. **CUET:** Экзамен для поступления в университеты страны, начиная с 2022 года. Он был введен как единый экзамен для студентов, желающих учиться в государственном и частном секторе высшего образования. **UGC NET:** Экзамен для кандидатов, желающих стать преподавателями в высших учебных заведениях, а также для тех, кто хочет пройти аспирантуру в области гуманитарных, социальных и естественных наук.

NTA активно использует технологии для повышения эффективности экзаменационного процесса. Среди значимых инноваций стоит отметить:

- **Интернет-платформы и онлайн-экзамены:** NTA внедрила систему онлайн-подачи заявок, а также электронных тестов и многократных повторных экзаменов для повышения доступности.
- **Меры безопасности:** Для предотвращения нарушений и мошенничества на экзаменах используются различные технические средства, включая сканеры для проверки документов, видеонаблюдение и биометрические системы для идентификации кандидатов.
- **Электронные результаты и обратная связь:** Результаты экзаменов публикуются в онлайн-режиме, что позволяет кандидатам быстро получить информацию и ознакомиться с анализом своей работы.