

Protecting Hotel Computer Networks from External Denial-of-Service Threats

Assist. Prof. PhD Stefka Petrova
University of Economics - Varna, Varna, Bulgaria
s.petrova@ue-varna.bg

PhD candidate Dimitrios Simeonidis
University of Economics - Varna, Varna, Bulgaria
simeonidis@ue-varna.bg

Abstract

The study examines the growing threat of DoS/DDoS attacks against hotel computer networks, which are highly dependent on uninterrupted access to reservation systems, payments and internet services for guests. The aim is to propose an effective, multi-layered approach to prevent, detect and mitigate these attacks. Hotel networks are vulnerable due to their public nature (for example guest Wi-Fi) and limited IT resources. DoS attacks can block critical services, resulting in the inability to process reservations, payments and accommodation, causing not only financial losses but also a lot of reputational damage. Traditional defense mechanisms (simple firewalls) are often insufficient against today's high-volume DDoS attacks. An integrated approach based on several key methods is proposed. Successful protection requires a combination of on-premises network measures and powerful open-source tools. Hotels should accept the DoS threat as an operational risk and implement proactive, scalable solutions to ensure the continuity of their critical services and maintain customer trust.

Keywords: hotel cybersecurity; network security; DoS attack; Hotel networks

JEL Code: C88, L86

DOI: 10.56065/IJUSV-ESS/2025.14.2.58

Въведение

С развитието на глобалната мрежа интернет, зависимостта от информационните системи, използващи компютърни мрежи нараства значително. Мрежите вече не са изолирани инфраструктури, а взаимосвързани системи, поддържащи финансови трансакции, комуникации и множество други услуги. Въпреки безспорното удобство, тази зависимост води и до повишен риск от външни, за една организация, киберзаплахи.

Видовете външни заплахи обикновено в литературата се разделят в следните основни групи (Jonu & Namim 2023):

- Вируси и злонамерен софтуер (Malware) – програми, които се инсталират без знанието на потребителя и могат да откраднат информация, да унищожат данни или да предоставят достъп на трета страна;
- Фишинг атаки – социално-инженерни техники, целящи измама на потребителя с цел предоставяне на лични данни или пароли;
- SQL инжекции и уеб експлойти – използват слабости в уеб приложенията за извличане или модифициране на бази данни;
- MITM (Man-in-the-Middle) – прихващане на комуникацията между две страни с цел шпиониране или подмяна на данни;
- Zero-day уязвимости – неизвестни за производителите слабости в софтуера, които се използват от нападателите, преди да бъдат коригирани;
- DoS и DDoS (Denial of Service, Distributed Denial of Service) – атаки (може и разпределени от множество източници) от тип отказ на обслужване, които претоварват мрежата с фалшив трафик, водещ до срив на услугите.

В настоящата публикация се разглеждат основните аспекти на последната спомената киберзаплаха във връзка със сигурността на компютърните мрежи, както и методите и

технологииите за тяхната защита. Особено внимание се отделя на стратегическия подход за изграждане на устойчива система за защита, която ефективно да комбинира технически, организационни и човешки фактори.

1. Основни видове атаки от тип отказ на обслужване

DoS атаките са специфичен вид киберзаплаха, използвана за прекратяване на нормалната работа на мрежа, услуга или система чрез изпращане на голям обем мрежови трафик или голям брой клиент-сървър заявки. По този начин атаката лишава целевата система от възможност да обслужва легитимни потребители. Последиците от тези атаки са значителни: те могат временно да спрат услугата, да причинят финансови проблеми и да навредят на репутацията на атакуваната организация. Съществен проблем са някои IoT устройства, които имат ниско ниво на сигурност и могат да бъдат използвани за формиране на ботнет мрежи (Alabsi et al. 2023). Този проблем е установен сравнително отдавна в доклад на Kaspersky, където се посочва, че честотата на DoS атаките се е увеличила рязко поради появата на несигурни IoT устройства (Gupta & Badve 2017).

В сравнение с DoS атаките, DDoS атаките са по-сложни, тъй като използват множество компютри, принадлежащи най-често към ботнет мрежи, специално предназначени за атака на целевата система и в процеса ескалират мащаба на атаката (Eliyan & Di Pietro 2021). Организаторите на атаката в повечето случаи контролират голям брой компрометирани компютри (т.нар. „зомбита“), с които могат да стартират едновременна атака срещу една система. В някои случаи междинните мрежови устройства – рутери и други системи предназначени за предаване, разпределяне и обработка на трафика, се претоварват от големия обем трафик, а не самата информационна система, която е и крайната цел, но това също постига целите на DoS атаката (Shurman et al. 2020).

Има няколко основни категории DoS атаки в зависимост от това дали са ориентирани към протокол или метод. По-долу са систематизирани някои от по-често срещаните видове DoS атаки и техните последици за достъпността на мрежата:

- TCP SYN Flood – един от най-разпространените видове DoS атаки. Тя се възползва от настройка на механизма за „ръкостискане“ (handshaking) на TCP протокола. В обичаен TCP процес на ръкостискане, клиентите изпращат SYN съобщение със заявка до сървъра, а сървърът връща SYN-ACK съобщение. Нападателят генерира голям брой SYN заявки и никога не ги потвърждава, като по този начин принуждава сървъра да установява и поддържа полуотворени връзки. Тъй като сървърът, трябва да използва част от своята памет и процесорно време, за да поддържа съответната връзка, сървърът се претоварва и се достига до отказ на обслужване на легитимните клиенти (Kim et al. 2020).

- UDP Flood – за разлика от TCP, който е ориентиран към предварително осигуряване на мрежова връзка, UDP не изисква предварително „ръкостискане“ преди да се обменят данни. Извършва се изпращане на голям обем UDP пакети към всеки порт на целевата система. Целевата система се опитва да обработи всеки пакет, получен по UDP, като изпраща ICMP - Destination Unreachable уведомителни съобщения, което води до изчерпване на ресурсите и прекъсване на услугите. Тази атака може да бъде стартирана сравнително лесно, оставяйки анализаторите ѝ безпомощни да се справят с проблема (Prasad et al. 2014).

- ICMP Flood (Ping of Death) – изпращат се възможно най-много ICMP Echo Request пакети (pings) към целевата система. Обикновено броя на изпратените ping пакети за единица време е по-голям от това, което системата може да обработи, и целта ще спре да отговаря. Някои автори посочват, че Ping of Death е доста прост тип атака, която не изисква атакуващият да е професионален хакер, но ако са замесени множество устройства, които да извършват тази атака, тя оказва значително въздействие на системите (Kurniawan et al. 2021).

- HTTP Flood – атаката се извършва чрез изпращане на привидно нормални HTTP GET или POST заявки до уеб сървър. Уеб сървърът трябва да обработва всяка заявка, но няма

капацитет да отговори на всички тези заявки едновременно и по този начин започва да забавя отговорите си или дори блокира. Повечето реални HTTP Flood атаки не използват фалшиви IP адреси, както при TCP SYN Flood или UDP Flood атаките и техните пакети не са изкуствено променени, което означава, че откриването и предотвратяването на HTTP Flood атаки е сравнително трудно (Alabsi et al. 2023).

- Slowloris – атакуващ инициира голям брой връзки към целевия уеб сървър, но изпраща данни с много бавна скорост. Докато сървърът чака да се осъществи връзката и изпратят данните, други заявки от легитимни клиенти не могат да бъдат обработени своевременно. Според някои автори атаката е по-ефективна срещу уеб сървъри, базирани на нишки (Kim et al. 2020).

Посочените атаки използват различни протоколи по нива на модела OSI, но всички работят в посока на претоварване на целевата система, като същевременно се отказва услуга на реалните потребители (Gniewkowski 2020; Simeonidis et al. 2023).

2. Варианти за противодействие на DoS атаки

Ефектът от прилагане на DoS атаките се изразява най-вече в намаляване на времето за нормална комуникация по мрежата като се претоварва пропускателната способност на канала за връзка, процесорна мощност или памет, за да предотврати достъпа на истинските потребители до необходимите мрежови услуги. За бизнеса това може да доведе до загуба на продажби, недоволство на клиентите и накърняване на имиджа на организацията (Ghali et al., 2020; Panayotova et al. 2016). Особено в индустрии с критична инфраструктура, като здравеопазване или финанси, въздействието на киберзаплахите може да доведе до критични обстоятелства, включително заплахи за живота или смущения в бизнеса (Chenniappanadar et al. 2022; Malkawi et al. 2021).

Следва да се има предвид, че освен да създават прекъсване на услугата, DoS атаките може да служат за прикриване на други злонамерени действия, които могат да се извършат паралелно. Когато атакуваната организация се концентрира върху елиминирането на DoS атаката, нападателите могат да се опитат да получат неоторизиран достъп до други системи или да получат поверителна информация, т.е. DoS атаките може да се комбинират като съставна част от по-големи и по-сложни кибератаки (Kurniawan et al. 2021).

Тъй като DoS и DDoS атаките представляват значителна заплаха за компютърните мрежи и системи, редица автори предлагат различни контрамерки за предотвратяване на подобни атаки. Тези контрамерки могат да бъдат класифицирани като превантивни, детективни и адаптивни (Galeano-Brajones et al. 2020):

- Ограничаване на скоростта – превантивен механизъм, чрез който се пропуска само количеството трафик, което сървърът може да получи от произволен източник за даден период от време. Чрез предотвратяване получаването на голям брой заявки за единица време, идващи от един IP адрес, се минимизира потенциалът за успешна DoS атака. Ограничаването на скоростта не работи ефективно срещу DDoS атаки, при които източниците на трафик са множество (Shurman et al. 2020).

- IP черен списък – достъпът от известни IP адреси, които са злонамерени, се забранява. Черните списъци може да бъдат статични, където записите се добавят, променят и изтриват ръчно, или динамични, където записите се актуализират автоматично. Този подход може да помогне срещу много DoS атаки, но той не работи ефективно срещу DDoS атаки, особено тези, включващи множество компрометирани устройства с различни IP адреси (Alabsi et al. 2023).

- Центрове за пречистване на трафика (traffic scrubbing center) – използват се за филтриране на лошия трафик, преди той да стигне до целевата система. Центровете за пречистване се използват често в големи организации и организации, предоставящи облачни услуги. Тези центрове изучават входящия трафик и спират лошите пакети, докато добрите се

пропускат. Центровете за пречистване са най-ефективни за масови DDoS атаки, тъй като филтрирането в периферията на мрежата е недостатъчно (Kurniawan et al. 2021).

- Използване на системи за откриване и предотвратяване на прониквания от тип **Intrusion Detection and Prevention System (IDPS)** – тези системи наблюдават мрежовия трафик и предупреждават администраторите за активност, която може да е признак за атаки. Техниките за машинно обучение (Kostadinova et al. 2023) могат да допълнят работата на IDPS, за да идентифицират моделите на активност, типични за DoS атаките (Garcia & Blandon 2022). Такива системи може да използват модели за дълбоко обучение, включително CNN и LSTM, за да класифицират сложния модел на злонамерен трафик (Shurman et al. 2020).

3. Системи за откриване и предотвратяване на прониквания

Системите за откриване и предотвратяване на прониквания от тип IDPS имат за цел да наблюдават и анализират мрежовия трафик или дейностите на хостовете, за да откриват признаци на неоторизиран достъп, нарушения на данните или атаки от типа „отказ на услуга“ (DoS атаки) (Pundir et al. 2020). Тяхната роля е от съществено значение за защитата на компютърните системи, особено когато традиционните механизми за сигурност, като защитни стени и антивирусни инструменти, са недостатъчни за справяне с напреднали, динамични заплахи. Те се използват главно като бариера за защита на мрежата от кибернахлувания чрез идентифициране на различни нередности, преди да причинят сериозни щети на мрежата, като предоставят на организациите откриване в реално време и ранна защита, давайки възможност да смекчат заплахите, преди те да се разширят (Bhati et al. 2020; Simeonidis et al. 2024).

IDPS има четири ключови компоненти – механизми за откриване, които проверяват трафика за подозрителна активност; механизми за генериране на предупреждения, които информират за вероятни нарушения на сигурността; механизми за реагиране, които могат да неутрализират трафика, който е нарушил сигурността, или да изолират компрометирани системи. Допълнително, IDPS може да бъде включена в други общи системи за сигурност, за да осигури наблюдение в реално време и да подобри откриването (Landauer et al. 2022).

Съществува разделение в IDPS според вида технология, която използват за откриване на прониквания и тяхното позициониране в дадената мрежа:

- Мрежово базирани IDPS (Network Intrusion Detection and Prevention System, NIDPS) – работят в реално време, като следят пакетите с данни и изследват потока от пакети за такива с определени инкриминиращи характеристики. Работи на специално предназначени устройства, които са разположени на стратегически места в мрежата. NIDPS е ефикасен при идентифициране на DoS атаки, IP spoofing и сканиране на портове (Al-Janabi et al. 2021). Предимствата на NIDPS включват, че NIDPS може да открива множество устройства едновременно, без да влошава производителността на мрежата (Pundir et al. 2020).

- Хост базирани IDPS (Host-Based Intrusion Detection and Prevention System, HIDPS) – за разлика от NIDPS, HIDPS работи на всеки целеви хост в мрежата. Извършва се проверка на лог файлове, събрани от системата, състоянието на различни приложения на хоста, както и анализ на файлове за признаци на нелегитимна манипулация на конкретен хост. Това, което прави HIDPS по-ефективен, е, че може да открива вътрешни заплахи или атаки, които често остават незабелязани, защото по някакъв начин заобикалят мрежовите слоеве. Основен недостатък на HIDPS обаче е, че използването му може да причини изчерпване на системни ресурси, като по този начин възпрепятства производителността (Ghawade 2021).

- Хибридна IDPS (Hybrid Intrusion Detection and Prevention System) – комбинирано използване на NIDPS и HIDPS, тъй като двете имат различна ефективност при справяне с различни ситуации. Комбинира се наблюдението на трафика на ниво цялата мрежа с изследване на трафика на ниво хост, като по този начин се предоставят редица възможности за идентифициране на заплахи. Някои изследвания сочат, че хибридната IDPS предлага

необходимата устойчивост, адаптивност и покритие за защита както на границите на мрежата, така и на конкретни хостове (Kishore & Chauhan 2020).

4. Организация на работа по защита на хотелска компютърна мрежа

Публикацията NIST Special Publication 1800-27 (SP 1800-27) – “Securing Property Management Systems” представлява практическо ръководство, разработено от Националния институт по стандарти и технологии на САЩ (NIST), което е предназначено към повишаване на киберсигурността в хотелската индустрия чрез защита на Системите за управление на собствеността (Property Management Systems, PMS). Тези системи, понякога наричани и Системи за управление на хотели (Hotel Operating System, HOS), интегрират функционалности за резервации, плащания, управление на достъпа и обмен на клиентски данни, което ги прави критична точка за атаки.

В контекста на DoS (Denial of Service) и DDoS (Distributed Denial of Service) атаки, SP 1800-27 предоставя рамка за изграждане на устойчива, сегментирана и контролирана мрежова архитектура, която намалява риска от претоварване на PMS инфраструктурата. Документът акцентира върху няколко ключови направления, релевантни към защитата срещу DoS атаки:

- Мрежова сегментация и Zero Trust принципи – чрез разделяне на хотелската ИТ инфраструктура на зони (например PMS, IoT устройства, гост мрежа и административен сегмент) се предотвратява хоризонталното разпространение на атаки. Zero Trust моделът, препоръчан от NIST, елиминира „доверие по подразбиране“, като изисква непрекъсната автентикация и мониторинг на всички връзки.

- Мониторинг и откриване на аномалии – SP 1800-27 препоръчва използването на системи за откриване на опити за мрежови аномалии от тип IDPS и централизирани системи за управление на информация и събития за сигурност от тип SIEM (Security Information and Event Management) за анализ на трафика. Това позволява ранно откриване на модели, характерни за DoS атаки – като необичайно висока честота на заявки или нетипичен източник на трафик.

- Управление на достъпа и контрол на капацитета – чрез прилагане на ролево базирани права за достъп и ограничаване на комуникационните канали, PMS-сървърите могат да са по-малко уязвими на претоварване. Механизмите за капацитетно управление (rate limiting, throttling) намаляват въздействието на DoS атаки.

- Облачна и хибридна устойчивост – SP 1800-27 препоръчва интеграция на PMS с облачни услуги, които разполагат с вградени защити срещу DDoS атаки (например CDN и load-balancing системи).

- Инциденти и възстановяване – SP 1800-27 дефинира процедурна рамка за реакция при инциденти, включваща откриване, ограничаване, анализ и възстановяване. При DoS атаки това означава изолиране на засегнатите сегменти, пренасочване на трафика и използване на резервни комуникационни канали.

Приложението на тези мерки в хотелски контекст позволява на организациите не само да ограничат риска от срив на PMS и свързаните услуги, но и да гарантират непрекъснатост на бизнес процесите и доверие на клиентите. SP 1800-27 може да служи като практически инструмент за изграждане на архитектура, устойчива на DoS и други киберзаплахи.

5. Защита на компютърна мрежа чрез използване на софтуерни инструменти с лиценз свободен софтуер

Една типична хотелска локална компютърна мрежа е необходимо да има следните основни компоненти: централен файървол (защитна стена) на връзката с интернет; DMZ зона (DeMilitarized Zone) за публично достъпни услуги като уебсървъри, пощенски и др. сървъри; Вътрешни LAN сегменти за различни отдели (например: финанси, ЧР, администрация, гости);

VPN за дистанционен достъп на служителите; IDPS система за наблюдение на трафика. Тази структура позволява изолация на рисковете и по-добър контрол върху достъпа.

Нашите изследвания сочат, че подходящи софтуерни инструменти от тип IDPS с лиценз свободен софтуер са Snort и Suricata, които могат да се използват в различни ситуации.

Таблица 1. Сравнение на някои параметри на системите Snort и Suricata.

Показател	Snort	Suricata
Архитектура	Версия 2 е еднонишкова и може да бъде по-ефективна по отношение на ресурсите при системи с ниска производителност. Може да се използва и под Windows Версия 3 е многонишкова.	Многонишкова, проектирана за среди с висок трафик.
Производителност	По-ниско системно натоварване при системи с едно ядро.	По-висока производителност на модерен хардуер с многоядрен процесор.
Инспекция на пакети	Базови възможности за дълбока проверка на пакети (DPI).	По-добри възможности за дълбока проверка на пакети (DPI).
Дневници (logs)	Традиционни формати за регистриране.	Поддържа гъвкави формати за регистриране, включително JSON.
Съвместимост на правилата	Използва предимно собствен формат на правилата, но много правила са съвместими със Suricata.	Използва както собствен формат на правилата, така и може да използва повечето правила на Snort с корекции.
Пример за употреба	Версия 2 подходяща за по-малки мрежи, домашни среди или среди с ограничена процесорна мощност.	Мащабни корпоративни среди, мрежи с висока пропускателна способност.
Общност и поддръжка	Голяма и утвърдена общност с обширна документация и поддръжка.	Активна общност, но Snort има по-дълга история с по-голяма ресурсна база.

След сваляне и инсталиране е необходимо да се зададат правилни настройки в конфигурационните файлове (например, къде да се съхранява лог-файла) и да се свалят актуални правила, чрез които се проверява мрежовия трафик. Правила за Suricata и Snort за различни версии на тези продукти може да се свалят от <https://rules.emergingthreats.net/open/>. Работата с продуктите е с интерфейс команден ред. За работа с графичен потребителски интерфейс може да се използват продукти, базирани на Suricata, като SELKS (старо наименование на продукта) / Clear NDR Community (ново наименование на продукта). NDR е съкратено от Network threat Detection and Response. Последните версии на продуктите към момента на извършване на проучването са SELKS 10 (пусната 13.06.2024 г.) и Clear NDR 1.0 (пусната 10.09.2025 г. - <https://www.stamus-networks.com/clear-ndr-community>).

Освен Snort и Suricata, като системи за откриване и предотвратяване на проникване може да се използват и други инструменти с отворен код: Zeek (преди известен като Bro) или Wazuh. Като система от тип HIDPS може да се използва OSSEC, която следи системни файлове, логове и регистри за необичайна активност. Интерес представлява платформата с

множество възможности Security Onion – дистрибуция на Linux с отворен код, която интегрира Suricata, Snort, Zeek и други инструменти за сигурност в един лесен за управление пакет. По този начин предоставя цялостно решение за мониторинг и анализ.

Заклучение

Предпазването на компютърна мрежа от външни заплахи е процес, който изисква последователност на мерките, постоянство, комплексен подход и адаптивност. В условията на бързо развиваща се дигитална среда, където атаките стават все по-автоматизирани и интелигентни, традиционните методи за защита вече не са достатъчни. Необходимо е комбинирано прилагане на технологии, политики и човешки фактор - изграждане на култура на сигурност, комбинирана с модерни инструменти за мониторинг, криптиране и управление на достъпа. В бъдеще ще се развият адаптивни системи, които не просто реагират на атаки, а ги предвиждат и предотвратяват проактивно. Само чрез цялостен и гъвкав подход може да се осигури устойчива защита на мрежовата инфраструктура и да се гарантира сигурността на данните в дигиталната ера.

References

1. Alabsi, B., Anbar, M., & Rihan, S. (2023). Conditional Tabular Generative Adversarial Based Intrusion Detection System for Detecting Ddos and Dos Attacks on the Internet of Things Networks. *Sensors*, 23(12). DOI: <https://doi.org/10.3390/s23125644>
2. Bhati, N., Khari, M., Díaz, V., & Verdú, E. (2020). A Review on Intrusion Detection Systems and Techniques. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 28, 65-91. DOI: <https://doi.org/10.1142/s0218488520400140>
3. Chenniappanadar, S., Sundharamurthy, G., Sakthivelu, V., & Kaliappan, V. (2022). A Supervised Machine Learning Based Intrusion Detection Model for Detecting Cyber-Attacks Against Computer System. *International Journal of Communication Networks and Information Security (IJCNIS)*, 14, 16-25. DOI: <https://doi.org/10.17762/ijcnis.v14i3.5567>
4. Eliyan, L. F., & Di Pietro, R. (2021). DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. *Future Generation Computer Systems*, 122, 149-171. DOI: <https://doi.org/10.1016/j.future.2021.03.011>
5. Galeano-Brajones, J., Carmona-Murillo, J., Valenzuela-Valdés, J. F., & Luna-Valero, F. (2020). Detection and mitigation of DoS and DDoS attacks in IoT-based stateful SDN: An experimental approach. *Sensors*, 20(3), 816. DOI: <https://doi.org/10.3390/s20030816>
6. Garcia, J., & Blandon, G. (2022). A Deep Learning-Based Intrusion Detection and Prevention System for Detecting and Preventing Denial-of-Service Attacks. *IEEE Access*, 10, 83043-83060. DOI: <https://doi.org/10.1109/access.2022.3196642>
7. Ghali, A., Ahmad, R., & Alhussian, H. (2020). Comparative analysis of DoS and DDoS attacks in Internet of Things environment. In *Artificial Intelligence and Bioinspired Computational Methods: Proceedings of the 9th Computer Science On-line Conference 2020*, Vol.29, Springer International Publishing, pp.183-194. DOI: https://doi.org/10.1007/978-3-030-51971-1_15
8. Ghawade, M. (2021). Study of Intrusion Detection System. *International Journal for Research in Applied Science and Engineering Technology*, 9(VI) DOI: <https://doi.org/10.22214/IJRASET.2021.34935>
9. Gniewkowski, M. (2020). An overview of DoS and DDoS attack detection techniques. In *International Conference on Dependability and Complex Systems*. Cham: Springer International Publishing, pp.233-241. DOI: https://doi.org/10.1007/978-3-030-48256-5_23
10. Gupta, B. B., & Badve, O. P. (2017). Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a cloud computing environment. *Neural Computing and Applications*, 28, 3655-3682. DOI: <https://doi.org/10.1007/s00521-016-2317-5>

11. Jony, A. I., & Hamim, S. A. (2023). Navigating the Cyber Threat Landscape: A Comprehensive Analysis of Attacks and Security in the Digital Age. *Journal of Information Technology and Cyber Security*, 1(2), pp.53-67. DOI: <https://doi.org/10.30996/jitcs.9715>
12. Kim, J., Kim, J., Kim, H., Shim, M., & Choi, E. (2020). CNN-Based Network Intrusion Detection against Denial-of-Service Attacks. *Electronics*, 9(6), 916. DOI: <https://doi.org/10.3390/electronics9060916>
13. Kishore, R., & Chauhan, A. (2020). Intrusion Detection System a Need. *2020 IEEE International Conference for Innovation in Technology (INOCON)*, Bangluru, India, pp.1-7. DOI: <https://doi.org/10.1109/INOCON50539.2020.9298398>
14. Kostadinova, I., Dimitrov, G., Martsenyuk, V., Rancic, D., Dirgova-Luptakova, I., Jovancevic, I., ... (2023). Research and Analysis of IT Specifications of Good Practices in the Area of Artificial Intelligence. In *2023 16th International Conference on Advanced Technologies, Systems and Services in Telecommunications (TELSIKS)*, IEEE, pp.284-290. DOI: <https://doi.org/10.1109/TELSIKS57806.2023.10316145>
15. Kurniawan, A., Jusak, J., & Musayyanah, M. (2021). Intrusion Detection System Using Deep Learning for DoS Attack Detection. *JEECS (Journal of Electrical Engineering and Computer Sciences)*, 6(2), pp.1087-1098. DOI: <https://doi.org/10.54732/jeeecs.v6i2.203>
16. Landauer, M., Skopik, F., Frank, M., Hotwagner, W., Wurzenberger, M., & Rauber, A. (2022). Maintainable Log Datasets for Evaluation of Intrusion Detection Systems. *IEEE Transactions on Dependable and Secure Computing*, 20, 3466-3482. DOI: <https://doi.org/10.1109/TDSC.2022.3201582>
17. Malkawi, R., Alsmadi, I., Aleroud, A., & Petrov, P. (2021). A firewall-adversarial testing approach for software defined networks. *Journal of Theoretical and Applied Information Technology*, 99(1), pp.227-241.
18. National Institute of Standards and Technology (2021). *Securing Property Management Systems*. NIST SP 1800-27. [Online] Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-27.pdf> [Accessed 28/10/2025]
19. Panayotova, G., Dimitrov, G., Petrov, P., Bychkov, O. (2016). Modeling and data processing of information systems. *3rd International Conference on Artificial Intelligence and Pattern Recognition (AIPR)*, Lodz, Poland, IEEE, pp.1-5. DOI: <https://doi.org/10.1109/ICAIPR.2016.7585229>
20. Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS attacks: defense, detection and traceback mechanisms-a survey. *Global Journal of Computer Science and Technology*, 14(7), pp.15-32.
21. Pundir, S., Lee, S., Kim, D., & Kim, J. (2020). Intrusion detection system. *International Journal of Engineering and Techniques*, 6(4). DOI: <https://doi.org/10.29126/23951303/ijet-v6i4p7>
22. Shurman, M., Khrais, R., & Yateem, A. (2020). DoS and DDoS attack detection using deep learning and IDS. *International Arab Journal of Information Technology*, 17(4A, Special Issue), pp.655-661. DOI: <https://doi.org/10.34028/iajit/17/4a/10>
23. Simeonidis, D., Petrov, P., Jordanov, J. (2023). Network Intrusion Detection Through Classification Methods and Machine Learning Techniques. *International Conference Automatics and Informatics (ICAI)*, IEEE, pp.409-413. DOI: <https://doi.org/10.1109/ICAI58806.2023.10339029>
24. Simeonidis, D., Petrov, P., Penchev, G., Petrova, S., Dimitrov, G., Petrivskiy, V. (2024) Performance and Accuracy Assessment of Detecting Network Intrusions with eSOM-Based Techniques. *International Conference Automatics and Informatics (ICAI)*, IEEE, pp.586-591. DOI: <https://doi.org/10.1109/ICAI63388.2024.10851699>