

Статья поступила в редакцию: 13.08.2026

Статья принята к публикации: 15.09.2026

Статья опубликована: 28.09.2026

УДК 004.7

Топологии и защита информации

Сухачёв Никита Алексеевич

студент кафедры информационной безопасности Технологический университет

имени А.А. Леонова

Российская Федерация, г. Королёв

E-mail: brawl.sukh@mail.ru

Теребина Анна Александровна

Студентка кафедры информационной безопасности Технологический университет

имени А.А. Леонова

Российская Федерация, г. Королёв

E-mail: ANNA.TEREBINA@yandex.ru

Topologies and information security

Sukachev Nikita Alekseevich

student, Department of Information Security Leonov Technological University

Russia, Korolev

Terebina Anna Aleksandrovna

student, Department of Information Security Leonov Technological University

Russia, Korolev

Аннотация

В современном мире, где информация стала одним из самых ценных ресурсов, её защита — не просто техническая задача, а вопрос выживания бизнеса и доверия пользователей. Каждый день мы слышим о новых кибератаках, утечках данных и сбоях в работе критически важных систем — и всё это напоминает: уязвимость может скрываться не только в коде или настройках, но и в самой архитектуре сети. Именно поэтому вопрос выбора правильной топологии нельзя считать второстепенным: от того, как соединены узлы, напрямую зависит, насколько надёжно будут храниться и передаваться данные. В данной работе рассматривается влияние топологии компьютерной сети на уровень защищённости информации. Проведён сравнительный анализ четырёх базовых топологий («шина», «кольцо», «звезда», «смешанная») по таким критериям, как конфиденциальность, целостность, доступность, устойчивость к отказам, масштабируемость и сложность обнаружения вторжений. Для количественной оценки уязвимостей предложена авторская модель расчёта коэффициента защиты информации (КЗИ), основанная на методологии

ФСТЭК. Результаты расчёта показывают, что наилучшую защищённость обеспечивает смешанная топология ($KЗИ = 0,14$), а топология «звезда» ($KЗИ = 0,34$) является оптимальным выбором для большинства корпоративных сетей.

Abstract

In today's world, where information has become one of the most valuable resources, its protection is not merely a technical task but a matter of business survival and user trust. Every day we hear about new cyberattacks, data leaks, and failures in critical systems — all of which remind us that vulnerabilities may reside not only in code or configuration settings but also in the network architecture itself. That is why the choice of the right topology cannot be considered secondary: the reliability of data storage and transmission directly depends on how the nodes are interconnected. This paper examines the influence of computer network topology on the level of information security. A comparative analysis of four basic topologies — bus, ring, star, and hybrid — was conducted based on such criteria as confidentiality, integrity, availability, fault tolerance, scalability, and intrusion detection complexity. To quantitatively assess vulnerabilities, the authors propose an original model for calculating the information protection coefficient (IPC), grounded in the methodology of the Russian Federal Service for Technical and Export Control (FSTEC). The calculation results show that the hybrid topology provides the highest level of protection ($IPC = 0.14$), while the star topology ($IPC = 0.34$) represents the optimal choice for most corporate networks.

Ключевые слова: топология сети, защита информации, коэффициент защиты информации, ФСТЭК, смешанная топология, отказоустойчивость, компьютерные сети.

Keywords: network topology, information security, Information Protection Coefficient, FSTEC, hybrid topology, fault tolerance, computer networks.

Введение

Топология компьютерной сети — это схема соединения устройств: «шина», «звезда», «кольцо» или «смешанная». Она определяет, как данные передаются между узлами, что напрямую влияет на скорость, надёжность и удобство обслуживания. Однако существует ещё один важный параметр, который редко связывают с топологией, — безопасность. В корпоративной среде защиту информации чаще всего строят на криптографии, контроле доступа и мониторинге трафика. Однако на практике уязвимости могут быть заложены уже на уровне физической схемы соединений [1]. Актуальность исследования обусловлена необходимостью количественной оценки влияния архитектурных особенностей сети на её защищённость. Методика анализа защищённости информационных систем (утверждена Федеральной службой по техническому и экспортному контролю 25 ноября 2025 г.) задаёт общие требования к оценке защищённости, однако не рассматривает топологию сети как самостоятельный фактор. В существующих научных работах топологии рассматриваются преимущественно с точки зрения производительности и отказоустойчивости [2], тогда как аспект безопасности остаётся недостаточно изученным [4].

Цель исследования — провести сравнительный анализ топологий компьютерных сетей по показателям безопасности и эксплуатационным характеристикам и разработать количественную модель оценки их защищённости.

Материалы и методы

В работе рассмотрены четыре базовые топологии компьютерных сетей: «шина», «кольцо», «звезда» и «смешанная» (гибридная). Для сравнительного анализа использованы три группы показателей:

Группа 1 — показатели безопасности (табл. 1)

1. Конфиденциальность — возможность несанкционированного перехвата данных.
2. Живучесть при повреждении — способность сохранять работоспособность при отказе отдельных элементов.
3. Защита от сетевых атак типа «отказ в обслуживании» (DDoS).
4. Наличие единой точки отказа.
5. Масштабируемость — возможность расширения сети без существенного снижения характеристик.
6. Сложность обнаружения вторжений.

Группа 2 — эксплуатационные характеристики (табл. 2)

1. Производительность.
2. Задержка передачи данных.
3. Гибкость конфигурации.
4. Помехозащищённость.
5. Сложность обнаружения и локализации неисправностей.

Группа 3 — группы угроз (табл. 3)

1. Перехват трафика.
2. Отказ канала связи.
3. DDoS-атака.
4. Компрометация узла.
5. Единая точка отказа.

Для оценки топологий применяются три методики.

Методика 1 — качественная оценка показателей безопасности и эксплуатационных характеристик (табл. 1 и 2). Каждый показатель оценивается по шкале уровней: «низкий», «средний», «высокий». Оценка отражает степень выраженности соответствующего свойства топологии.

Методика 2 — количественная интерпретация качественных оценок. Уровням присваиваются числовые значения: «низкий» — 1, «средний» — 2, «высокий» — 3. Итоговая оценка топологии по группе показателей определяется как среднее арифметическое значений по соответствующим показателям. Чем выше итоговая оценка, тем лучше характеристика топологии.

Методика 3 — количественная оценка групп угроз по интервальной шкале коэффициента уязвимости от 0 до 1. Каждой угрозе присваивается коэффициент уязвимости:

- 0 — угроза полностью отсутствует;
- 0,1–0,3 — низкая уязвимость;
- 0,4–0,6 — средняя уязвимость;
- 0,7–0,9 — высокая уязвимость.

Значения коэффициентов определены экспертным путём на основе анализа архитектурных особенностей каждой топологии [10, 5]. КЗИ рассчитывается как среднее арифметическое всех коэффициентов уязвимости для каждой топологии. Чем меньше значение КЗИ, тем выше защищённость.

Во всех трёх методиках итоговая оценка топологии определяется как среднее арифметическое значений по соответствующим показателям. Весовые коэффициенты не применяются.

Результаты и обсуждения

Для количественного и наглядного сравнения уязвимостей различных топологий сведём их ключевые характеристики в таблицу 1.

Таблица 1.

Сравнение характеристик топологий (показатели безопасности)

Показатель	Шина	Кольцо	Звезда	Смешанная
Конфиденциальность	Низкая. Данные передаются по общей среде, каждый узел физически может принимать весь трафик сегмента [1].	Средняя. Трафик проходит последовательно через все узлы, что теоретически позволяет перехватывать пакеты при компрометации узла [5].	Высокая. Коммутатор направляет трафик только порту назначения, остальные узлы не видят чужие данные (при отсутствии атак на коммутатор)[3].	Высокая. Используются сегментированные звёзды; трафик внутри сегмента изолирован [6].
Живучесть при повреждении	Низкая. Разрыв общего кабеля в любой точке приводит к потере связи между всеми узлами [2].	Низкая. Разрыв кольца размыкает цепь, сеть распадается на два изолированных сегмента [2].	Высокая. Повреждение кабеля между коммутатором и одним узлом выводит из строя только этот узел [7].	Очень высокая. Отказ одного сегмента не влияет на остальные; критичные сегменты могут резервироваться [6].

Показатель	Шина	Кольцо	Звезда	Смешанная
Защита от DDoS	Низкая. Атака на один узел (например, генерация ложного трафика) может затопить всю шину и парализовать сеть [8].	Средняя. «Зашумление» одного узла нарушает передачу по всему кольцу, но маркерный доступ может частично ограничить влияние [5].	Высокая. Коммутатор может изолировать некорректный порт, локализуя атаку в пределах атакующего узла [7].	Высокая. Локализация атак внутри сегментов; центральные устройства мониторят аномалии [9].
Единая точка отказа	Весь кабель является распределённой точкой отказа — повреждение любого участка фатально [2].	Каждый узел и каждый кабель являются точкой отказа — выход одного узла разрывает кольцо [5].	Центральный коммутатор (или маршрутизатор) — если он выходит из строя, сеть полностью парализована [7].	Коммутаторы могут дублироваться, сохраняя работоспособность [9].
Масштабируемость	Крайне низкая. Добавление новых узлов увеличивает количество потенциальных «слушателей» и снижает надёжность шины [1].	Низкая. Добавление узла требует разрыва кольца, что временно останавливает всю сеть; растёт задержка [4].	Высокая. Новый узел подключается к свободному порту коммутатора без влияния на остальных [10].	Высокая. Расширение происходит путём добавления новых «звёзд» без изменения архитектуры [6].
Сложность обнаружения вторжений	Высокая. Отсутствие центрального управления затрудняет мониторинг; аномальный трафик сложно отличить от нормального [1].	Средняя. Возможен пассивный мониторинг, но локализация источника требует анализа на каждом узле [4].	Низкая. Коммутатор может зеркалировать порты, логировать подключения, быстро выявлять подозрительную активность [7].	Низкая. Централизованные коммутаторы и сегментирование позволяют строить эффективные системы обнаружения вторжений (IDS/IPS) [9].

Количественная интерпретация табл. 1 (Методика 2). Присвоим уровням числовые значения: «низкий» — 1, «средний» — 2, «высокий» — 3. Для показателя «Единая точка отказа» оценка инвертируется: отсутствие единой точки отказа — 3, наличие — 1. Результаты сведены в таблицу 2.

Таблица 2.

Количественная оценка показателей безопасности

Показатель	Шина	Кольцо	Звезда	Смешанная
Конфиденциальность	1	2	3	3
Живучесть при повреждении	1	1	3	3
Защита от DDoS	1	2	3	3
Единая точка отказа (инвертированная)	1	1	1	3
Масштабируемость	1	1	3	3
Сложность обнаружения вторжений (инвертированная)	1	2	3	3
Сумма	6	9	16	18
Среднее	1,00	1,50	2,67	3,00

Таким образом, по показателям безопасности наилучшей является смешанная топология (средняя оценка 3,00), на втором месте — «звезда» (2,67). Топологии «шина» (1,00) и «кольцо» (1,50) имеют неудовлетворительные показатели.

Таблица 3.**Сравнение дополнительных параметров (эксплуатационные характеристики)**

Параметр	Шина	Кольцо	Звезда	Смешанная
Производительность	Низкая. Общая шина — пропускная способность делится между всеми узлами. При росте сети скорость падает катастрофически [2].	Средняя. Данные идут по кругу, каждый узел создаёт микро-задержку. При большом количестве узлов падение скорости заметно [4].	Высокая. Каждый узел имеет выделенный канал до коммутатора. Производительность не падает при добавлении новых узлов (до заполнения портов) [10].	Высокая. Наследует от «звезды» внутри сегментов. При грамотном проектировании падения производительности нет [6].
Задержка передачи данных	Высокая. При коллизиях узлы ждут случайное время и повторяют отправку. Непредсказуемая задержка [2].	Средняя. Пакет проходит последовательно через все узлы, пока не дойдёт до адресата. Задержка растёт с каждым новым узлом [4].	Низкая. Коммутатор получает пакет и мгновенно отправляет только на порт назначения. Задержка минимальна и стабильна [7].	Низкая. В пределах сегмента — как у «звезды». При передаче между сегментами задержка чуть выше, но не критично [6].
Гибкость конфигурации	Очень низкая. Любое изменение требует остановки всей сети и физического вмешательства в общий кабель [1].	Низкая. Добавление или удаление узла требует разрыва кольца и остановки сети. Перенастройка сложная [4].	Высокая. Новый узел подключается к свободному порту коммутатора на ходу. Удаление узла — просто отключить кабель. Сеть продолжает работать [7].	Высокая. Каждый сегмент (отдельная «звезда») настраивается независимо. Можно менять конфигурацию одного сегмента без остановки других [9].
Помехозащищённость	Низкая. Длинный общий кабель работает как антенна. Наводки на одном участке могут исказить сигнал для всех узлов [2].	Средняя. Сигнал регенерируется каждым узлом при передаче дальше, что «очищает» его от помех. Но сам кабель длинный [5].	Высокая. Кабель от коммутатора до узла — отдельная линия. Помеха на одном кабеле не влияет на другие узлы [7].	Высокая. Наследует от «звезды». Каждый сегмент защищён от помех в других сегментах [9].
Сложность обнаружения и локализации неисправностей	Сложная. Обрыв кабеля где-то на шине парализует всю сеть, но понять, в каком именно месте обрыв, трудно. Нужно смотреть каждый участок [1].	Сложная. Сеть разорвана, но неясно, какой именно узел или кабель сломался. Приходится проверять каждый узел и каждый соединительный отрезок [4].	Простая. Коммутатор обычно имеет световую индикацию или интерфейс управления, показывающие, какой порт не работает. Можно быстро заменить кабель или узел [10].	Средняя. При отказе одного сегмента остальные работают. Но локализация требует проверки коммутаторов каждого сегмента по очереди [9].

Количественная интерпретация табл. 3 (Методика 2). Присвоим уровням числовые значения: «низкий» — 1, «средний» — 2, «высокий» — 3. Для параметров «Задержка передачи данных» и «Сложность обнаружения и локализации неисправностей» оценка инвертируется: чем ниже задержка и чем проще обнаружение, тем выше балл. Результаты сведены в таблицу 4.

Таблица 4.**Количественная оценка эксплуатационных характеристик**

Параметр	Шина	Кольцо	Звезда	Смешанная
Производительность	1	2	3	3
Задержка передачи данных (инвертированная)	1	2	3	3
Гибкость конфигурации	1	1	3	3
Помехозащищённость	1	2	3	3
Сложность обнаружения и локализации неисправностей (инвертированная)	1	1	3	2
Сумма	5	8	15	14
Среднее	1,00	1,60	3,00	2,80

Таким образом, по эксплуатационным характеристикам наилучшей является топология «звезда» (средняя оценка 3,00), на втором месте — смешанная топология (2,80). Топологии «шина» (1,00) и «кольцо» (1,60) имеют неудовлетворительные показатели.

Сопоставление результатов по табл. 2 и 4. Смешанная топология лидирует по показателям безопасности (3,00), но немного уступает «звезде» по эксплуатационным характеристикам (2,80 против 3,00). Топология «звезда» обеспечивает наилучшие эксплуатационные характеристики и высокие показатели безопасности (2,67), уступая смешанной только по отказоустойчивости и наличию единой точки отказа. Топологии «шина» и «кольцо» существенно уступают по обеим группам показателей [2, 10].

Расчёт коэффициента защиты информации (КЗИ)

Для количественной оценки защищённости каждой топологии разработана авторская модель на основе интервальной шкалы коэффициента уязвимости от 0 до 1 (Методика 3). В предлагаемой модели каждой топологии ставится в соответствие набор коэффициентов уязвимости по нескольким группам угроз, выделенным на основе анализа архитектурных особенностей [5, 9].

Таблица 5.**Оценка уязвимости топологий по группам угроз**

Группа угроз	Шина	Кольцо	Звезда	Смешанная	Обоснование
Перехват трафика	0,9	0,6	0,2	0,1	В «шине» все узлы видят весь трафик; в «кольце» — при компрометации узла; в «звезде» трафик изолирован; в «смешанной» — сегментирован [1, 3].

Группа угроз	Шина	Кольцо	Звезда	Смешанная	Обоснование
Отказ канала связи	0,9	0,8	0,3	0,2	Общий кабель «шины» и «кольца» критичен; в «звезде» отказ только одного узла; в «смешанной» — резервирование [2, 7].
DDoS-атака	0,8	0,5	0,2	0,1	«Шина» парализуется полностью; «кольцо» — частично; «звезда» — коммутатор изолирует порт; «смешанная» — сегментация [8, 9].
Компрометация узла	0,5	0,7	0,1	0,1	В «кольце» каждый узел является ретранслятором; в «шине» — пассивное прослушивание; в «звезде» и «смешанной» — влияние минимально [3, 5].
Единая точка отказа	0,9	0,8	0,9	0,2	«Шина» — весь кабель; «кольцо» — любой узел; «звезда» — центральный коммутатор; «смешанная» — дублирование [2, 7].

Расчёт КЗИ (среднее арифметическое)

1. Шина: $KZI = (0,9 + 0,9 + 0,8 + 0,5 + 0,9) / 5 = 0,80$
2. Кольцо: $KZI = (0,6 + 0,8 + 0,5 + 0,7 + 0,8) / 5 = 0,68$
3. Звезда: $KZI = (0,2 + 0,3 + 0,2 + 0,1 + 0,9) / 5 = 0,34$
4. Смешанная: $KZI = (0,1 + 0,2 + 0,1 + 0,1 + 0,2) / 5 = 0,14$

Сводная таблица результатов

Таблица 6.

Сводные результаты оценки топологий

Топология	Средняя оценка по показателям безопасности (табл. 1а)	Средняя оценка по эксплуатационным характеристикам (табл. 2а)	КЗИ (табл. 3)	Топология
Шина	1,00	1,00	0,80	Шина
Кольцо	1,50	1,60	0,68	Кольцо
Звезда	2,67	3,00	0,34	Звезда

Полученные значения КЗИ отражают интегральную оценку уязвимости каждой топологии. Результаты расчёта показывают, что наилучшую защищённость обеспечивает смешанная топология ($KZI = 0,14$). На втором месте — топология «звезда» ($KZI = 0,34$). Топологии «шина» и «кольцо» имеют неудовлетворительные показатели (0,80 и 0,68 соответственно), что подтверждает их нецелесообразность для построения защищённых сетей [1, 2, 9]. Сопоставление результатов по трём методикам показывает, что смешанная топология обеспечивает наиболее высокий уровень безопасности (средняя оценка 3,00 по табл. 1а, $KZI = 0,14$). Топология «звезда» является оптимальным выбором для большинства корпоративных сетей по соотношению «безопасность / стоимость»: она обеспечивает наилучшие эксплуатационные характеристики (3,00) и высокие показатели безопасности

(2,67) при приемлемом КЗИ (0,34). Топологии «шина» и «кольцо» уступают по всем трём группам показателей и не рекомендуются для использования в современных корпоративных сетях [2, 10, 6].

Заключение

В результате проведённого исследования были получены следующие выводы:

1. Качественный анализ показал, что топологии «шина» и «кольцо» обладают критическими уязвимостями: низкой конфиденциальностью, наличием распределённой единой точки отказа и сложностью обнаружения вторжений. Количественная оценка подтвердила это: средние оценки по показателям безопасности составили 1,00 и 1,50 соответственно, по эксплуатационным характеристикам — 1,00 и 1,60, КЗИ — 0,80 и 0,68. Данные топологии не рекомендуются для использования в современных корпоративных сетях.

2. Топология «звезда» обеспечивает высокую производительность, низкие задержки, гибкость, хорошую помехозащищённость и простоту обнаружения неисправностей. Её единственным существенным недостатком является единая точка отказа — центральный коммутатор, который может быть защищён резервированием. Средняя оценка по показателям безопасности — 2,67, по эксплуатационным характеристикам — 3,00, КЗИ — 0,34.

3. Смешанная топология наследует преимущества «звезды» внутри сегментов и обеспечивает дополнительную отказоустойчивость за счёт сегментации и возможности резервирования критичных компонентов. Средняя оценка по показателям безопасности — 3,00, по эксплуатационным характеристикам — 2,80, КЗИ — 0,14.

4. Количественный расчёт КЗИ с использованием авторской модели на основе интервальной шкалы коэффициента уязвимости подтвердил, что смешанная топология является наиболее защищённой (КЗИ = 0,14), а топология «звезда» (КЗИ = 0,34) — оптимальным выбором для большинства корпоративных сетей по соотношению «безопасность / стоимость».

5. Наиболее высокий уровень безопасности обеспечивает смешанная топология. Полученные результаты могут быть использованы при проектировании защищённых корпоративных сетей и выборе архитектуры, обеспечивающей требуемый уровень безопасности при минимальных затратах на дополнительные средства защиты.

Список литературы

1. Методика анализа защищённости информационных систем: утверждена Федеральной службой по техническому и экспортному контролю 25 ноября 2025 г. – Москва: ФСТЭК России, 2025.
2. Монахова, Э.А., Монахов, О.Г. О некоторых характеристиках циркулянтных и тороидальных структур вычислительных систем // Вестник СибГУТИ. – 2022. – № 4.
3. An Investigation into the Performance of DHKE Algorithm over Different Network Topologies in Cryptography Networks // Proceedings of the. – 2023. – P. 1–6. – DOI: 10.1109/ICISCT60174.2023.10390219.

4. ChameleonNet: Topology Obfuscation Against Tomography With Critical Information Hiding // IEEE Transactions on Networking. – 2025. – Т. 33, № 5. – P. 2585–2600. – DOI: 10.1109/TON.2025.11006136.
5. Heidari Safari, M.E., Hosseini, S. A federated framework for simulating and predicting malware propagation in network topologies with privacy awareness // Scientific Reports. – 2026. – DOI: 10.1038/s41598-026-69350-4.
6. Hettiarachchi, E.D. S.I., Sarkar, N.I., & Gutierrez, J. Impact of Southbound Expansion on Clustered OpenFlow Software-Defined Network Controller Synchronisation Using ODL and ONOS // Information. – 2024. – Т. 15, № 8. – DOI: 10.3390/info15080440.
7. Li, X., Lee, J., Son, J. & Lee, Y. Tunnel enabled programmable switches obfuscate network topology to defend against link flooding reconnaissance in software defined networking // Scientific Reports. – 2025. – Т. 15.
8. Protection Mechanism Against Internal Data Leakage Based on Scitags // Proceedings of the. – 2025. – P. 1–8. – DOI: 10.1109/NAS63823.2025.11181425.
9. Reducing Mean Absolute Error in Attack Predictions With Power-Parametrized Choquet Integrals // ITL – International Journal of Applied Information Technology. – 2026. – DOI: 10.1002/itl2.70368.
10. Thaenchakun, S., Kanjanasit, K. Evaluation of Secured and Unsecured OSPF Routing Protocols: A Simulated Experiment // East African Journal of Information Technology. – 2026. – Т. 9, № 1. – DOI: 10.37284/eajit.9.1.4536.

References

1. [Methodology for analyzing the security of information systems]: approved by the Federal Service for Technical and Export Control on November 25, 2025. Moscow, FSTEC Rossii Publ., 2025. (In Russ.)
2. Monakhova E.A., Monakhov O.G. [On some characteristics of circulant and toroidal structures of computing systems]. Vestnik SibGUTI, 2022, no. 4. (In Russ.)
3. An Investigation into the Performance of DHKE Algorithm over Different Network Topologies in Cryptography Networks // Proceedings of the. – 2023. – P. 1–6. – DOI: 10.1109/ICISCT60174.2023.10390219.
4. ChameleonNet: Topology Obfuscation Against Tomography With Critical Information Hiding. IEEE Transactions on Networking, 2025, vol. 33, no. 5, P. 2585–2600. DOI: 10.1109/TON.2025.11006136.
5. Heidari Safari M.E., Hosseini S. A federated framework for simulating and predicting malware propagation in network topologies with privacy awareness. Scientific Reports. – 2026. – DOI: 10.1038/s41598-026-69350-4.
6. Hettiarachchi E.D.S.I., Sarkar N.I., Gutierrez J. Impact of Southbound Expansion on Clustered OpenFlow Software-Defined Network Controller Synchronisation Using ODL and ONOS. Information, 2024, vol. 15, no. 8, P. 440. DOI: 10.3390/info15080440.

7. Li X., Lee J., Son J., Lee Y. Tunnel enabled programmable switches obfuscate network topology to defend against link flooding reconnaissance in software defined networking. Scientific Reports, 2025, vol. 15.
8. Protection Mechanism Against Internal Data Leakage Based on Scitags // Proceedings of the. – 2025. – P. 1–8. – DOI: 10.1109/NAS63823.2025.11181425.
9. Reducing Mean Absolute Error in Attack Predictions With Power-Parametrized Choquet Integrals. ITL – International Journal of Applied Information Technology. – 2026. – DOI: 10.1002/itl2.70368.
10. Thaenchakun S., Kanjanasit K. Evaluation of Secured and Unsecured OSPF Routing Protocols: A Simulated Experiment. East African Journal of Information Technology, 2026, vol. 9, no. 1. DOI: 10.37284/eajit.9.1.4536.