Чернівецький національний університет імені Юрія Федьковича

Навчально-науковий інститут фізико-технічних та комп'ютерних наук

Кафедра комп'ютерних систем та мереж

"ЗАТВЕРДЖУЮ"
Директор навчально-наукового інституту
фізико-технічних та комп'ютерних наук
_____ **Петро ШПАТАР**
"31" серпня 2026 року

РОБОЧА ПРОГРАМА
навчальної дисципліни

ВК3 Захист комп'ютерних мереж
(назва навчальної дисципліни)

вибіркова
(вказати: обов'язкова / вибіркова)

Освітньо-професійна програма Комп'ютерна інженерія
(назва програми)

Спеціальність F7 Комп'ютерна інженерія
(вказати: код, назва)

Галузь знань F Інформаційні технології
(вказати: шифр, назва)

Рівень вищої освіти другий (магістерський)
(вказати: перший бакалаврський/другий магістерський)

фізико-технічних та комп'ютерних наук
(назва факультету/ навчально-наукового інституту,
на якому здійснюється підготовка фахівців за вказаною освітньо-професійною програмою)

Мова навчання українська

Чернівці 2026 рік

Робоча програма навчальної дисципліни «Захист комп'ютерних мереж» складена відповідно до освітньо-професійної програми «Комп'ютерна інженерія».

Розробник: Танасюк Юлія Володимирівна, доцент кафедри КСМ, канд. фіз.-мат. наук, доцент
(П.І.Б. авторів, посада, науковий ступінь, вчене звання)

Викладач (чі), що забезпечує читання даної навчальної дисципліни:
Танасюк Юлія Володимирівна, доцент кафедри КСМ, канд. фіз-мат. наук, доцент
(П.І.Б. викладача (ів), посада, науковий ступінь, вчене звання)

Затверджено на засіданні кафедри *комп'ютерних систем та мереж*

Протокол № 2 від "31" серпня 2026 року

Завідувач кафедри _____ **Георгій ВОРОБЕЦЬ**
(підпис)

Схвалено методичною радою навчально-наукового інституту фізико-технічних та комп'ютерних наук

Протокол № 1/2 від "31" серпня 2026 року

Голова методичної ради навчально-наукового інституту фізико-технічних та комп'ютерних наук

_____ **Іван КОЗЯРСЬКИЙ**
(підпис)

1. Мета навчальної дисципліни

Мета: полягає у формуванні у студентів системного розуміння принципів забезпечення безпеки комп'ютерних систем і мереж та набутті практичних навичок застосування сучасних механізмів захисту, контролю доступу, фільтрації трафіку, криптографії, хмарної безпеки та моніторингу подій безпеки. У результаті вивчення дисципліни здобувачі освіти опанують знання та навички роботи з основними підходами та механізмами захисту систем і мереж, налаштування локального та серверного контролю доступу, розширеного застосування списків контролю доступу для фільтрації трафіку, конфігурування брандмауерів і зональних політик безпеки, визначення вимог до захисту хмарних середовищ, вибору криптографічних методів для забезпечення конфіденційності, цілісності та автентичності даних, а також використання журналів, мережних даних і сповіщень для моніторингу та оцінювання подій інформаційної безпеки.

2. Результати навчання

Вивчення навчальної дисципліни сприяє формуванню у здобувачів вищої освіти таких компетентностей:

ЗК – загальних

ЗК1. Здатність до адаптації та дій в новій ситуації.
ЗК2. Здатність до абстрактного мислення, аналізу і синтезу.
ЗК4. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
ЗК7. Здатність приймати обґрунтовані рішення.
ЗК8. Здатність спілкуватися іноземною мовою.

СК – фахових (спеціальних)

СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.
СК4. Здатність будувати та досліджувати моделі комп'ютерних систем та мереж.
СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів.
СК11. Здатність обирати ефективні методи розв'язування складних задач комп'ютерної інженерії, критично оцінювати отримані результати та аргументувати прийняті рішення.

РН - програмних результатів навчання

РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.
РН3. Будувати та досліджувати моделі комп'ютерних систем і мереж, оцінювати їх адекватність, визначати межі застосовності.
РН5. Розробляти і реалізовувати проєкти у сфері комп'ютерної інженерії та дотичні до неї міждисциплінарні проєкти з урахуванням інженерних, соціальних, економічних, правових та інших аспектів.

РН6. Аналізувати проблематику, ідентифікувати та формулювати конкретні проблеми, що потребують вирішення, обирати ефективні методи їх вирішення.
РН8. Застосовувати знання технічних характеристик, конструктивних особливостей, призначення і правил експлуатації програмно-технічних засобів комп'ютерних систем та мереж для вирішення складних задач комп'ютерної інженерії та дотичних проблем.
РН11. Приймати ефективні рішення з питань розроблення, впровадження та експлуатації комп'ютерних систем і мереж, аналізувати альтернативи, оцінювати ризики та імовірні наслідки рішень.
РН13. Зрозуміло і недвозначно доносити власні знання, висновки та аргументацію з питань інформаційних технологій і дотичних міжгалузевих питань до фахівців і нефахівців, зокрема до осіб, які навчаються.

У результаті вивчення навчальної дисципліни «Захист комп'ютерних мереж» здобувачі освіти повинні продемонструвати такі навчальні досягнення:

Знати:

- методи захисту мережної інфраструктури, кінцевих пристроїв і серверів від несанкціонованого доступу, шкідливого програмного забезпечення та мережних атак;
- принципи керування доступом до мережних ресурсів, механізми автентифікації, авторизації та обліку дій користувачів (AAA), технології 802.1X, EAP і MAB;
- призначення, принципи функціонування та особливості налаштування списків контролю доступу (ACL), міжмережних екранів і політик фільтрації мережевого трафіку;
- призначення, архітектуру та принципи функціонування систем виявлення і запобігання вторгненням (IDS/IPS), засобів захисту кінцевих пристроїв і систем моніторингу безпеки;
- основні механізми захисту хмарної інфраструктури, особливості керування доступом, захисту даних і мережних ресурсів у хмарних середовищах;
- принципи централізованого керування мережевою безпекою, зокрема призначення Cisco ISE, технологій Cisco TrustSec та механізмів динамічного призначення політик доступу;
- методи моніторингу стану мережевої безпеки, збирання й аналізу журналів подій, мережевого трафіку та сповіщень про потенційні загрози;
- основні підходи до оцінювання ризиків, виявлення інцидентів інформаційної безпеки та визначення пріоритетів реагування на загрози.

Вміти:

- аналізувати архітектуру комп'ютерних мереж, визначати потенційні вразливості, оцінювати загрози та обґрунтовувати вибір заходів захисту;
- налаштовувати механізми контролю доступу до мережевих пристроїв, серверів і ресурсів, застосовувати принципи AAA та технології автентифікації користувачів і кінцевих пристроїв;
- розробляти й налаштовувати розширені списки контролю доступу (ACL), правила міжмережних екранів і політики фільтрації трафіку відповідно до заданих вимог безпеки;

- налаштовувати засоби захисту кінцевих пристроїв і застосовувати механізми виявлення та блокування шкідливої активності;
- обирати та застосовувати криптографічні механізми для забезпечення конфіденційності, цілісності й автентичності інформації;
- налаштовувати механізми мережної автентифікації на основі 802.1X, EAP і RADIUS, застосовувати засоби централізованого керування доступом, зокрема Cisco ISE, та політики групового доступу з використанням Cisco TrustSec;
- збирати й аналізувати журнали подій, мережевий трафік і сповіщення систем безпеки для виявлення підозрілої активності та потенційних інцидентів;
- інтерпретувати результати моніторингу безпеки, визначати ознаки атак і порушень політик доступу, оцінювати критичність виявлених подій.

3. Опис навчальної дисципліни

3.1. Загальна інформація

Форма навчання	**Рік підготовки**	**Семестр**	**Кількість**		**Кількість годин**						**Вид підсумкового контролю**
			кредитів	**всього годин**	**лекції**	**практичні**	**семінарські**	**лабораторні**	**самостійна робота**	**індивідуальні завдання**	
Денна	1(5)	2(10)	3	90	14	-	-	16	60	-	Залік
Заочна	1(5)	2(10)	3	90	2	-	-	4	84	-	Залік

3.2. Структура змісту навчальної дисципліни

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 1. Багатошаровий захист розподілених систем та мереж												
Тема 1. Аспекти захисту комп'ютерних систем та мереж.	19	3	-	4	-	12	21,5	0,5	-	1	-	20
Тема 2. Методи та засоби контролю доступу. Технології брандмауерів і зональні політики безпеки.	26	4	-	4	-	18	23,5	0,5	-	1	-	22
Разом за змістовим модулем 1	45	7	-	8	-	30	90	2	-	4	-	84

Назви змістових модулів і тем	Кількість годин											
	Денна форма						Заочна форма					
	усього	у тому числі					усього	у тому числі				
		л	п	лаб	інд	с.р.		л	п	лаб	інд	с.р.
1	2	3	4	5	6	7	8	9	10	11	12	13
Змістовий модуль 2. Аналіз даних для виявлення потенційних загроз												
Тема 3. Безпека хмарних сховищ	22	3	-	4	-	15	21,5	0,5		1		20
Тема 4. Моніторинг безпеки. Системи журналювання даних та оповіщення про загрози.	23	4	-	4	-	15	23,5	0,5	-	1	-	22
Разом за змістовим модулем 2	45	7	-	8	-	30	90	2	-	4	-	84
Усього годин	**90**	**14**	**-**	**16**	**-**	**60**	**90**	**2**	**-**	**4**	**-**	**84**

Тематика лекційних занять з переліком питань

№	Назва теми з основними питаннями
Змістовий модуль 1. Багатошаровий захист розподілених систем та мереж	
1	**Захист комп'ютерних систем та мереж.** Розуміння захисту. Ешелонована оборона. Керування операціями з кібербезпеки. Фізична безпека. Безпека застосунків. Стандарти і та протоколи для підсилення безпеки. Захист бездротових та мобільних пристроїв.
2	**Контроль доступу.** Концепції контролю доступу. Керування обліковими записами. Засоби автономного адміністративного доступу. Структура AAA. Централізований контроль доступу на основі серверів RADIUS і TACACS+.
3	**Фільтрування даних.** Концепції контролю доступу. Керування обліковими записами. Розширені можливості списків контролю доступу. ACL для IPv6. Пом'якшення атак за допомогою ACL.
4	**Технології брандмауера.** Міжмережні екрани в плануванні мережі. Типи брандмауерів. Традиційна архітектура безпеки. Багатошаровий захист. Політики безпеки на основі зон (ZBP). Створення правил для опрацювання трафіку. Функціонування та налаштування ZBP.
Змістовий модуль 2. Аналіз даних для виявлення потенційних загроз	
5	**Безпека хмарних сховищ.** Віртуалізація та хмарні обчислення. Домени хмарної безпеки. Безпека хмарної інфраструктури, даних, віртуальних машин.
6	**Технології та протоколи безпеки.** Моніторинг стандартних протоколів DNS, SNMP, NTP, HTTP, HTTPs, ICMP, протоколи електронної пошти.
7	**Аналіз даних про стан безпеки.** Шифрування, інкапсуляція, тунелювання. Розподіл навантаження. Однорангові мережі та циклічна маршрутизація. Сповіщення безпеки. Журналювання даних. Netflow, Tcpdump, NGFW, Snort. Джерела сповіщень. Оцінювання сповіщень. Рівні небезпеки.

3.3. Тематика лабораторних занять

№	Назва теми (завдання)	Кількість годин денна/заочна ф.н.
Змістовий модуль 1. Основні концепції динамічної маршрутизації та політик захисту у корпоративних мережах		
1.	Запровадження параметрів безпеки на ключових вузлах у мережі	2/0,5
2.	Керування адміністративним доступом. Автентифікація на основі серверів RADIUS і TACACS+	4/0,5
3.	Розширені можливості списків контролю доступу	4/0,5
4.	Налаштування зональної політики (ZBP)	2/0,5
5.	Snort і правила брандмауера	4/2
	Разом:	16/4

3.4. Самостійна робота студента

№ з/п	**Назва теми**	Кількість годин денна/заочна ф.н.
1	Сучасні кіберзагрози та вектори атак: класифікація мережних атак, методи їх реалізації та підходи до протидії.	8/8
2	Криптографічні методи захисту інформації: симетричне й асиметричне шифрування, хешування, цифрові підписи, інфраструктура відкритих ключів (PKI).	10/12
3	Міжмережні екрани нового покоління (NGFW): архітектура, функціональні можливості, фільтрація трафіку та виявлення мережевих загроз.	6/10
4	Системи виявлення та запобігання вторгненням (IDS/IPS): принципи функціонування, методи виявлення атак, сигнатурний і поведінковий аналіз.	8/10
5	Захист кінцевих пристроїв: антивірусні технології, EDR/XDR, контроль цілісності, виявлення шкідливого програмного забезпечення та запобігання його поширенню.	8/12
6	Безпека бездротових мереж: механізми автентифікації та шифрування Wi-Fi, стандарти WPA2/WPA3, типові атаки на бездротову інфраструктуру та методи захисту.	6/10
7	Моніторинг мережної безпеки та керування інцидентами: аналіз журналів подій, SIEM-системи, кореляція подій, виявлення аномалій та етапи реагування на кіберінциденти	8/12
8	Аналіз вразливостей і тестування безпеки мереж: сканування портів і сервісів, оцінювання вразливостей, тестування на проникнення (Penetration Testing) та методи усунення виявлених недоліків.	6/10
	Разом:	60/84

4. Форми і методи навчання

Вивчення дисципліни «Захист комп'ютерних мереж» передбачає навчальні заняття у формі лекцій та лабораторних занять, виконання завдань із застосуванням комп'ютерної та телекомунікаційної техніки, а також використання програмного забезпечення з відкритим кодом та онлайн-доступом. Самостійна робота, пов'язана з опрацюванням теоретичного матеріалу та літературних джерел за відповідною тематикою, супроводжується формуванням напрацювань для подання та обґрунтування отриманих результатів виконання лабораторних завдань, підготовкою до контрольних робіт та тестів. Також під час проведення занять студенти залучені до виконання робіт на реальному мережному обладнанні та у симуляторі, беруть участь у обговореннях у малих групах, проєктному навчанні. У окремих випадках під час проведення занять використовуються мультимедійні засоби Google Meet і Cisco Webex і освітні платформи Moodle та netacad.com.

У межах дисципліни передбачено можливість використання результатів навчання, здобутих студентами під час проходження професійно-орієнтованих онлайн-курсів Cisco Networking Academy (NetAcad), зокрема Network Defense (українською мовою). Результати навчання, отримані поза межами формальної освітньої програми, можуть бути визнані відповідно до встановленого в університеті порядку за умови підтвердження їх успішного здобуття та відповідності програмним результатам навчання дисципліни.

Методи навчання: словесні (лекція, пояснення, дискусія, навчальна бесіда); наочні (демонстрація, ілюстрація, аналіз схем і моделей мережної інфраструктури); практичні (лабораторні роботи, практичні завдання, моделювання мережних атак і засобів захисту, аналіз мережного трафіку); проблемно-орієнтоване навчання; проєктне навчання; кейс-метод; дослідницький метод; кооперативне навчання; метод взаємного навчання й оцінювання.

5. Система контролю та оцінювання

Формами поточного контролю: усні відповіді студентів; обгрунтування реалізованих рішень, подання та аргументований захист результатів розв'язку практичних завдань у рамках колективного обговорення; виконання завдань проміжних та підсумкових контрольних робіт; результати складання тестів.

Підсумковий контроль – залік.

6. Критерії оцінювання поточного та підсумкового контролю

Поточне оцінювання (аудиторна та самостійна робота)						**Підсумковий контроль (залік)**	**Сумарна кількість балів**
Змістовий модуль 1			Змістовий модуль 2				
Т1	Т2	МК1	Т3	Т4	МК2	40	100
10	10	10	10	10	10		

Т1-Т4 – теми змістових модулів; МК1,2 – модульні контрольні роботи

Залежно від характеру відповіді здобувача освіти зазначена кількість балів може бути скоригована за наступними критеріями:

К-ть балів	**Критерії оцінки**
max	здобувач освіти дає вичерпну відповідь на поставлене запитання;
0,8 · max	здобувач освіти при відповіді на поставлене запитання припустився незначних неточностей, які не впливають на суть відповіді;
0,6 · max	здобувач освіти при відповіді на поставлене запитання припустився помилок, які виправляє за допомогою викладача; в середньому може дати правильні відповіді на 50% питань теми;
0,4 · max	здобувач освіти при відповіді на поставлене запитання припустився суттєвих помилок, які все ж таки виправляє за допомогою викладача; дає правильні відповіді на 30% питань теми;
0,2 · max	отримує здобувач освіти, який за допомогою викладача фрагментарно відповідає на запитання, проте не в повній мірі володіє мінімальним рівнем знань з даного питання;
0	якщо характер відповідей дає підставу стверджувати, що здобувач освіти неправильно зрозумів суть питання чи не знав правильної відповіді, а тому відповідав, припускаючись грубих помилок.

Примітка: за max прийнято максимальну оцінку для даного виду діяльності. Заокруглення проводиться до одиниць балу.

Згідно шкали ECTS загальна кількість балів, яку здобувач освіти може отримати у процесі вивчення дисципліни, становить 100 балів, з яких 60 балів здобувач освіти набирає при поточних видах контролю і 40 балів – у процесі підсумкового контролю (залік).

Шкала оцінювання: національна та ЄКТС

Оцінка за національною шкалою	**Оцінка за шкалою ЄКТС**	
	Оцінка (бали)	**Пояснення за розширеною шкалою**
Зараховано	A (90-100)	відмінно
	B (80-89)	дуже добре
	C (70-79)	добре
	D (60-69)	задовільно
	E (50-59)	достатньо
Не зараховано	FX (35-49)	(незадовільно) з можливістю повторного складання
	F (1-34)	(незадовільно)

		з обов'язковим самостійним повторним опрацюванням освітнього компонента до перескладання

7. Перелік питань для самоконтролю та підсумкового контролю навчальних досягнень здобувачів освіти

Змістовий модуль 1. Багатошаровий захист розподілених систем та мереж

1. Що таке багатошарова модель захисту (Defense in Depth) та які основні принципи її реалізації?
2. Які основні типи загроз і вразливостей характерні для сучасних розподілених систем та комп'ютерних мереж?
3. Які функції виконують міжмережні екрани та які існують основні типи брандмауерівl?
4. Які принципи побудови мережної сегментації та ізоляції ресурсів за допомогою VLAN і зон безпеки?
5. Яке призначення списків контролю доступу (ACL) та які особливості їх застосування для фільтрації мережного трафіку?
6. Які принципи автентифікації, авторизації та обліку дій користувачів реалізуються за допомогою моделі AAA?
7. Які механізми захисту мережевого доступу забезпечують технології 802.1X, EAP і RADIUS?
8. Які принципи функціонування систем виявлення та запобігання вторгненням IDS/IPS?
9. Які криптографічні механізми забезпечують конфіденційність, цілісність та автентичність інформації?
10. Які принципи побудови захищених VPN-з'єднань та чим відрізняються IPsec VPN і SSL/TLS VPN?
11. Які основні механізми захисту кінцевих пристроїв від шкідливого програмного забезпечення та несанкціонованого доступу?
12. Як реалізуються принципи Zero Trust та мікросегментації в сучасних корпоративних мережах?
13. Які основні механізми захисту хмарної інфраструктури та розподілених обчислювальних середовищ?
14. Які функції виконують системи централізованого керування мережною безпекою, зокрема Cisco ISE та Cisco TrustSec?
15. Як оцінити ефективність багатошарової системи захисту та визначити потенційні слабкі місця її архітектури?

Змістовий модуль 2. Аналіз даних для виявлення потенційних загроз

1. Які основні джерела даних використовуються для моніторингу стану мережної безпеки?
2. Охарактеризуйте методи збирання, фільтрації та попереднього оброблення даних застосовуються під час аналізу мережної активності.
3. Які типи мережного трафіку та поведінкових характеристик можуть свідчити про потенційну кібератаку?
4. Які принципи аналізу мережних пакетів і які можливості для цього надає Wireshark?
5. Які методи аналізу журналів подій використовуються для виявлення підозрілої активності?
6. Що таке SIEM-системи та які функції вони виконують у процесах моніторингу й аналізу подій безпеки?
7. Що таке кореляція подій безпеки та як вона допомагає виявляти складні багатоступеневі атаки?
8. Які методи виявлення аномалій у мережному трафіку застосовуються для ідентифікації потенційних загроз?
9. Чим відрізняються сигнатурний, поведінковий та евристичний методи виявлення загроз?
10. Які ознаки можуть свідчити про сканування портів, спроби несанкціонованого доступу, DoS/DDoS-атаки та поширення шкідливого програмного забезпечення?
11. Як використовуються системи IDS/IPS для аналізу мережного трафіку та виявлення ознак атак?
12. Які методи аналізу даних дають змогу виявляти аномальну поведінку користувачів і мережних пристроїв?
13. Яку роль відіграють методи машинного навчання та штучного інтелекту у виявленні кіберзагроз?
14. Як визначаються пріоритети оброблення сповіщень систем безпеки та оцінюється критичність виявлених подій?
15. Які основні етапи реагування на інциденти інформаційної безпеки та як результати аналізу даних використовуються для локалізації й усунення загроз?

8. Рекомендована література

Фахова (основна)

1. Кібербезпека : сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. / С. Е. Остапов, С. П. Євсеєв, О.Г. Король. Львів: «Новий Світ- 2000», 2024 . 678 с.
2. Молодший аналітик з кібербезпеки: Освітня траєкторія. URL: https://www.netacad.com/career-paths/cybersecurity?courseLang=uk-UA
3. Захист мережі. URL: https://www.netacad.com/courses/network-defense?courseLang=uk-UA
4. Захист інформації в комп'ютерних системах та мережах. Частина І: підручник / Ю.В. Костюк, П.М. Складанний. Київ : Київський столичний університет імені Бориса Грінченка, 2026. 401 с.
5. Бараннік Р. В. Кібербезпека і управління інформаційними ресурсами : навч. посіб. Київ : Юрінком Інтер, 2025. 236 с.
6. Терейковський, І. А. Захист інформації в комп'ютерних системах [Електронний ресурс] : навчальний посібник для здобувачів ступеня бакалавра за освітньою програмою «Системне програмування та спеціалізовані комп'ютерні системи» спеціальності 123 Комп'ютерна інженерія / І. А. Терейковський, С. О. Гнатюк ; КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, 2022. – 135 с.
7. Charlotte Magbanua Quiet Network, Safer Systems: A Practical Guide to Access Control, Segmentation, Monitoring , Incident Recovery, and Everyday Network Defense. 10BIL. 95 p.

Допоміжна

8. William Easttom. Network Defense and Countermeasures^ Principles and Practices. Pearson IT Certification. 2018. 544 p. URL: https://books.google.com.ua/books/about/Network_Defense_and_Countermeasures.html?id=_NFTDwAAQBAJ&redir_esc=y
9. Getting Started wit ATT&CK. URL: https://chatgpt.com/c/6ae319b8-dcf0-83ed-98d4-2a39fb6437e1
10. NIST Cybersecurity Framework (CSF) 2.0. 2024. URL: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-csf-20/final?utm_source
11. Wireshark: офіційна документація та посібник користувача. URL: https://www.wireshark.org/docs/
12. Security and VPN Configuration Guide. URL: https://www.cisco.com/c/en/us/td/docs/routers/ios-xe/security-vpn/security-vpn.html

Інформаційні ресурси

13. Security Onion Documentation. URL: https://docs.securityonion.net/en/3/dev/introduction/
14. Zeek Network Security Monitor Documentation. URL: https://docs.zeek.org/en/lts/
15. TryHackMe. URL: https://tryhackme.com/
16. NIST SP 800-207. Zero Trust Architecture. 2020. URL: https://www.nist.gov/publications/zero-trust-architecture