Google сервіси дозволяють освітянам, залежно від ситуації, ефективно співпрацювати та навчатися в різних режимах навчання (оф- чи онлайн), що особливо актуально в сучасних умовах. Важливим є те, що більшість Google сервісів є безкоштовними і відкритими для використання всіма користувачами, що робить їх доступними для широкого кола людей у всьому світі. Усі ці фактори роблять Google сервіси важливими інструментами для освіти.

Список використаних джерел

1. https://classroom.google.com/
2. https://www.smore.com/n/z69rg-educanon

Ящик О. Б.
кандидат педагогічних наук, доцент кафедри комп'ютерних технологій
Тернопільський національний педагогічний університет ім. В. Гнатюка,
м. Тернопіль, Україна

ОСОБЛИВОСТІ ФОРМУВАННЯ ЗНАНЬ ТА ВМІНЬ НАВЧАННЯ КІБЕРБЕЗПЕКИ СТУДЕНТІВ ІНЖЕНЕРНИХ СПЕЦІАЛЬНОСТЕЙ

Формування знань та вмінь у галузі кібербезпеки серед студентів інженерних спеціальностей є критично важливим завданням у сучасному світі, оскільки ця область стає все більш розгалуженою та складною. Розглянемо деякі особливості та методи, які можуть бути використані для ефективного формування знань та вмінь у цій сфері.

Інтерактивне навчання: використання інтерактивних методів навчання, таких як групові дискусії, кейс-стаді, та практичні вправи, дозволяє студентам отримувати практичний досвід та розвивати аналітичні навички. *Практичні завдання:* задачі, які вимагають від студентів вирішувати реальні проблеми з кібербезпекою, допомагають їм отримати реальний досвід та навички в роботі з системами безпеки. *Лабораторні роботи:* проведення лабораторних робіт, де студенти можуть експериментувати з різними аспектами кібербезпеки, такими як захист мережі, аналіз загроз, тестування на проникнення, дозволяє їм засвоювати теорію на практиці. *Курси з етики та законодавства:* важливо також надати студентам розуміння етичних та правових аспектів кібербезпеки, щоб вони розуміли відповідальність за свої дії в цій галузі. *Постійне оновлення матеріалів:* швидкий темп змін у галузі кібербезпеки вимагає постійного оновлення курсів та матеріалів навчання, щоб вони відображали найновіші технології та стратегії захисту. *Стажування та практичні проекти:* можливість проходження стажування в компаніях з кібербезпеки або участь у практичних проектах дозволяє студентам отримати реальний досвід роботи в цій галузі та побудувати мережу контактів. *Конкурси та змагання:* участь у конкурсах та змаганнях з кібербезпеки стимулює студентів до активного навчання та пошуку нових рішень у цій галузі. Важливою складовою є також підтримка та мотивація студентів, щоб вони були зацікавлені та активно займалися вивченням кібербезпеки.

Інтерактивне навчання в галузі кібербезпеки може включати широкий спектр методів, які сприяють активному залученню студентів у процес навчання та стимулюють їх аналітичне мислення та розв'язання проблем. Студенти можуть розділятися на групи та обговорювати актуальні питання з кібербезпеки, висловлювати свої думки щодо стратегій захисту та атак, а також аналізувати випадки порушень безпеки даних. Використання реальних кейсів або сценаріїв може допомогти студентам застосувати свої знання та вміння у вирішенні конкретних проблем з кібербезпеки, розробляти стратегії відновлення та захисту інформації. Влаштовування рольових ігор, де студенти можуть виконувати ролі хакера, адміністратора мережі, або експерта з безпеки, дозволяє їм поглибити своє розуміння процесів та проблем у сфері кібербезпеки. Студентам можуть пропонуватися завдання, які вимагають вирішення конкретних проблем з кібербезпеки, таких як виявлення вразливостей, аналіз логів безпеки, або відновлення після кібератаки. Використання спеціальних навчальних платформ або інструментів для проведення симуляцій кібератак та захисту дозволяє студентам отримати

практичний досвід роботи з різними аспектами кібербезпеки. Використання віртуальних лабораторних середовищ дозволяє студентам експериментувати з налаштуванням та тестуванням різних захисних механізмів без ризику для реальних систем. Проведення квізів та інтерактивних вправ під час лекцій або в онлайн-середовищах дозволяє перевіряти знання студентів та активізувати їх увагу під час навчання. Ці методи допомагають зробити процес навчання кібербезпеки більш цікавим, практичним та ефективним, дозволяючи студентам отримувати не лише теоретичні знання, але й реальний досвід роботи з проблемами безпеки в інтерактивному форматі.

Практичні завдання у галузі кібербезпеки відіграють важливу роль у формуванні навичок та здатностей студентів до ефективної роботи з захистом інформації та виявленням загроз. Студентам можуть бути надані віртуальні мережі або реальні тестові середовища для пошуку та аналізу вразливостей в мережевих пристроях та програмному забезпеченні. Студенти можуть бути запрошені до проведення тестування на проникнення в мережі чи системи за допомогою спеціальних інструментів та методів, щоб виявити та виправити потенційні вразливості. Студентам може бути надана інформація про реальні або симульовані кібератаки, і їм можуть ставитися завдання аналізувати дані журналів, визначати причини інциденту та розробляти плани відновлення. Студентам може бути надане завдання налаштувати різні захисні механізми в мережевих пристроях, встановити системи моніторингу та виявлення інцидентів, а потім провести моніторинг та аналіз потоків даних для виявлення загроз. Студентам може бути доручено розробити стратегії захисту для певної організації або мережі, враховуючи її конкретні потреби та загрози, та представити ці стратегії у вигляді презентацій або письмових звітів. Студенти можуть виконувати ролі атакувальників або оборонців під час симуляцій кібератак, щоб отримати реальний досвід в обох аспектах кібербезпеки. Ці практичні завдання допомагають студентам отримати практичний досвід роботи з реальними проблемами та сценаріями, з якими вони можуть зіткнутися у своїй майбутній професійній діяльності у сфері кібербезпеки.

Лабораторні роботи є ефективним способом навчання кібербезпеки, оскільки вони дозволяють студентам отримати практичний досвід роботи з реальними інструментами та технологіями. Студентам можуть бути надані віртуальні середовища з файерволами, де вони повинні налаштувати правила файервола для захисту мережі та проаналізувати журнали заборонених та дозволених пакетів. Студентам може бути надана можливість тестувати вразливості в реальних або симульованих веб-додатках, використовуючи різноманітні інструменти, такі як Burp Suite або OWASP ZAP. Студенти можуть аналізувати збір і аналіз мережевого трафіку з використанням інструментів, таких як Wireshark, для виявлення потенційно шкідливих або аномальних дій в мережі. Студентам може бути доручено налаштувати системи моніторингу безпеки, такі як системи виявлення вторгнень (IDS) або системи управління подіями та інцидентами (SIEM), і проаналізувати їхній вихідний потік для виявлення загроз. Студенти можуть відновлювати дані та системи після кібератаки, використовуючи різноманітні методи, такі як аналіз резервних копій, відновлення файлових систем тощо. Студенти можуть намагатися експлуатувати вразливості в реальних або симульованих системах, щоб отримати реальний досвід з проведення кібератак та розуміння захисних заходів. Ці лабораторні роботи дозволяють студентам отримати реальний досвід роботи з конкретними інструментами та технологіями, що використовуються у сфері кібербезпеки, та поглибити своє розуміння принципів захисту та атак.

Курси з етики та законодавства у сфері кібербезпеки важливі для того, щоб студенти розуміли етичні та правові аспекти своєї роботи, а також відповідальність, яку вони несуть у цій галузі. Огляд основних законів та нормативних актів, які стосуються кібербезпеки, таких як Закони про захист персональних даних, Закони про кіберзлочинність тощо. Розгляд етичних принципів, які повинні керувати діяльністю професіоналів у галузі кібербезпеки, таких як конфіденційність, цілісність та доступність даних. Розгляд понять відповідальності та обов’язку у сфері інформаційної безпеки, а також наслідків порушення етичних та правових

стандартів. Огляд міжнародних та національних стандартів безпеки інформації, таких як ISO 27001, та їх вплив на роботу у сфері кібербезпеки. Розгляд реальних випадків етичних конфліктів, з якими можуть стикатися фахівці з кібербезпеки, та способів їх вирішення. Огляд різних кодексів поведінки та професійних стандартів, які регулюють роботу фахівців у цій галузі. Ці курси допомагають студентам розуміти не лише технічні аспекти кібербезпеки, але й важливість етичного та правового підґрунтя їхньої діяльності. Вони допомагають сформувати етичність та професійність в студентів, що є ключовими якостями у сфері кібербезпеки.

Постійне оновлення матеріалів у навчанні кібербезпеки є критично важливим, оскільки ця галузь швидко змінюється і розвивається. Викладачі та навчальні заклади повинні слідкувати за останніми тенденціями, інцидентами та новинами в галузі кібербезпеки, щоб відразу включати актуальну інформацію в навчальні програми. Важливо встановлювати зв'язки з індустрією кібербезпеки, співпрацювати з компаніями та фахівцями, щоб отримувати першоджерела інформації про нові загрози та технології. Викладачі повинні користуватися актуальними джерелами інформації, такими як наукові журнали, конференції, веб-сайти професійних організацій та блоги експертів. Навчальні програми повинні бути гнучкими і здатними швидко адаптуватися до змін у галузі кібербезпеки, включаючи нові технології, методи атак та захисту. Використання онлайн-ресурсів, таких як відкриті курси, вебінари, онлайн-платформи для навчання та форуми, дозволяє отримувати доступ до актуальної інформації та ресурсів навчання. Студенти та колеги можуть бути важливим джерелом інформації про нові технології, методи та інші інновації у галузі кібербезпеки. Навчальні програми повинні регулярно оглядатися та оновлюватися для відображення найновіших тенденцій та вимог галузі кібербезпеки. Ці стратегії допомагають забезпечити, що навчальні матеріали в галузі кібербезпеки завжди залишаються актуальними та відповідають сучасним вимогам індустрії.

Стажування та практичні проекти грають важливу роль у навчанні кібербезпеки, оскільки вони надають студентам можливість отримати реальний досвід роботи в галузі та застосувати свої знання у практичних ситуаціях. Розглянемо кілька способів, які можуть бути використані для організації стажування та практичних проектів у кібербезпеці. Студенти можуть проходити стажування в компаніях, які спеціалізуються на кібербезпеці, де вони матимуть можливість працювати під керівництвом досвідчених фахівців та набувати практичний досвід роботи з реальними проектами. Університети можуть організовувати практичні проекти для студентів у співпраці з індустрією або у власних лабораторіях та дослідницьких центрах. Участь у змаганнях та хакатонах з кібербезпеки дозволяє студентам випробувати свої навички в реальних викликах та проблемах, а також отримати зворотний зв'язок від експертів. Студенти можуть вести самостійні дослідження та проекти в області кібербезпеки під керівництвом викладачів або менторів. Викладачі можуть організувати практичні вправи в класі, де студенти можуть розв'язувати конкретні завдання та сценарії з кібербезпеки. Університети можуть укладати партнерські угоди з урядовими організаціями або військовими структурами, щоб надати студентам можливість отримати практичний досвід у сфері кібербезпеки.

Ці форми стажування та практичних проектів допомагають студентам отримати практичний досвід роботи в галузі кібербезпеки, розвинути свої навички та навички, а також побудувати мережу контактів у цій сфері.

Конкурси та змагання у галузі кібербезпеки є важливими інструментами для розвитку навичок та виявлення талантів серед студентів та молодих фахівців. Вони стимулюють конкурентне середовище, сприяють обміну знаннями та навичками, а також відкривають можливості для співпраці та професійного зростання. Опишемо кілька типів конкурсів та змагань у цій галузі. Кіберзмагання (CTF): Capture The Flag (CTF) – це змагання, де учасники змагаються у вирішенні різних кібербезпекових завдань, таких як злам паролю, аналіз вразливостей, криптографія тощо. Це надає можливість випробувати та вдосконалити свої

технічні навички. Хакатони – це інтенсивні змагання, де учасники протягом обмеженого часу працюють у командах над розробкою рішень на базі конкретних технологічних викликів або проблем. Вони сприяють творчому мисленню та розвитку навичок роботи в команді. Конкурси з кібербезпеки для студентів, які дозволяють їм показати свої навички та знання у конкретних аспектах кібербезпеки. Вони можуть включати в себе вирішення завдань, тестування практичних навичок або розробку рішень. Змагання з робототехніки та Інтернету речей (IoT) спрямовані на розвиток навичок з області захисту вбудованих систем та пристроїв Інтернету речей, що стає все важливішим аспектом кібербезпеки. Змагання у вирішенні кібербезпекових викликів для підприємств можуть включати в себе симуляції кібератак або вирішення реальних викликів, що стикаються з підприємствами, що допомагає учасникам отримати реальний досвід роботи з кібербезпекою. Участь у таких конкурсах та змаганнях допомагає студентам та молодим фахівцям вдосконалити свої навички, показати свій потенціал та побудувати мережу контактів у галузі кібербезпеки.

У загальному висновку, навчання кібербезпеці для студентів інженерних спеціальностей є надзвичайно важливим і потребує комплексного підходу. Це включає в себе не лише технічні аспекти, такі як аналіз вразливостей та кібератаки, але й етичні, законодавчі та практичні аспекти.

Призначення курсів з етики та законодавства у сфері кібербезпеки допомагає створити свідомих фахівців, які розуміють важливість етичних та правових стандартів у їхній роботі. Практичні завдання, лабораторні роботи, стажування, практичні проекти та участь у конкурсах та змаганнях роблять навчання кібербезпеки більш ефективним та захопливим для студентів, надаючи їм можливість застосовувати свої знання на практиці та розвивати важливі навички.

Навчання кібербезпеці має бути постійно оновлюваним та адаптованим до змін у галузі, щоб гарантувати, що студенти отримують актуальні знання та навички, які потрібні для успішної кар’єри в цій сфері.

Загалом, інтеграція різноманітних методів навчання, від технічних до етичних, разом із практичними досвідом та участю у конкурсах, створює підґрунтя для успішного навчання та розвитку майбутніх фахівців з кібербезпеки.

Список використаних джерел:

1. Ящик О. Б., Симонов В. В., Іваненко Р. О. Забезпечення кібербезпеки в еру штучного інтелекту: аналіз технологічних підходів та стратегій для захисту інформації / БІЗНЕСІНФОРМ № 1_2024 // С. 81-86. DOI: https://doi.org/10.32983/2222-4459-2024-1-81-86

2. О. Б. Ящик, О. О. Олійник СТРУКТУРА ФАХОВИХ КОМПЕТЕНТНОСТЕЙ ІНЖЕНЕРІВ-ПЕДАГОГІВ / Зб. матер. ІІІ міжнар. конф. «Моделі міждисциплінарних та міжгалузевих освітніх та освітньо-наукових програм в умовах військового стану: виклики та варіанти впровадження»: 8-9 вересня 2023 р. / Одеський національний університет імені І. І. Мечникова. – Одеса, 2023. – 173-179 с.