**РЕКОМЕНДАЦІЇ ЩОДО ВИКЛАДАННЯ**

**КІБЕРБЕЗПЕКИ**

**2017 Р.**

Рекомендації щодо викладання кібербезпеки в рамках програм післяшкільної освіти

Посібник в рамках серії рекомендацій щодо викладання комп’ютерних наук

Спільна робоча група з питань освіти в галузі кібербезпеки

Асоціація обчислювальної техніки (Association for Computing Machinery, ACM)

Комп’ютерне товариство IEEE (IEEE Computer Society, IEEE-CS)

Спеціальна група з інформаційної безпеки та конфіденційності Асоціації інформаційних систем (Association for Information Systems Special Interest Group on Information Security and Privacy, AIS SIGSEC)

Технічний комітет з освіти в галузі інформаційної безпеки Міжнародної федерації з обробки інформації (International Federation for Information Processing Technical Committee on Information Security Education, IFIP WG 11.8)

Версія доповіді 1.0

31 грудня 2017 р.

**РЕКОМЕНДАЦІЇ ЩОДО ВИКЛАДАННЯ**

**КІБЕРБЕЗПЕКИ**

**2017 Р.**

Рекомендації щодо викладання кібербезпеки в рамках програм післяшкільної освіти

Посібник в рамках серії рекомендацій щодо викладання комп’ютерних наук

Спільна робоча група з питань освіти в галузі кібербезпеки

Асоціація обчислювальної техніки (Association for Computing Machinery, ACM)

Комп’ютерне товариство IEEE (IEEE Computer Society, IEEE-CS)

Спеціальна група з інформаційної безпеки та конфіденційності Асоціації інформаційних систем (Association for Information Systems Special Interest Group on Information Security and Privacy, AIS SIGSEC)

Технічний комітет з освіти в галузі інформаційної безпеки Міжнародної федерації по обробці інформації (International Federation for Information Processing Technical Committee on Information Security Education, IFIP WG 11.8)

Версія доповіді 1.0

31 грудня 2017 р.

© 2017 by ACM, IEEE, AIS, IFIP

ВСІ ПРАВА ЗАХИЩЕНО

Авторські права та дозвіл на передрук: дозвіл надається на використання цих рекомендації щодо викладання кібербезпеки для розробки навчальних планів і програм. Інше використання вимагає спеціального дозволу. Запити на дозвіл слід направляти за адресою: Відділ АСМ з надання дозволів (ACM Permissions Dept.), електронна пошта: permissions@acm.org, Керівник, відповідальний за авторські права IEEE (IEEE Copyrights Manager), електронна пошта: copyrights@ieee.org, AIS, електронна пошта: eLibrary@aisnet.org або IFIP, електронна пошта: ifip@ifip.org.

ISBN: 978-1-4503-5278-9

DOI: 10.1145/3184594

Веб-посилання: https://dl.acm.org/citation.cfm?id=3184594

Ви можете замовити додаткові копії за наявності за наступною адресою:

Відділ ACM з замовлень (ACM Order Department)

а/с 30777

Нью-Йорк, NY 10087-0777

Комп’ютерне товариство IEEE

Центр обслуговування клієнтів

10662 Лос Вакерос

а/с 3014

Лос Аламітос, CA 90720-1314

Спонсори:

Доповідь було підготовлено за фінансової підтримки наступних організацій:

Асоціація обчислювальної техніки (Association for Computing Machinery, ACM)

Комп’ютерне товариство IEEE (IEEE Computer Society, IEEE-CS)

Спеціальна група з інформаційної безпеки та конфіденційності Асоціації інформаційних систем (Association for Information Systems Special Interest Group on Information Security and Privacy, AIS SIGSEC)

Національний науковий фонд США (рішення № 1623104)

Корпорація Intel

Агентство національної безпеки США (Грант № H98230-17-1-0219)

Заключна доповідь з питань CSEC2017 була схвалена ACM, IEEE-CS, AIS SIGSEC і IFIP WG 11.8.

Дизайн обкладинки розроблено Nelly Group, LLC.

**РЕКОМЕНДАЦІЇ ЩОДО ВИКЛАДАННЯ**

**КІБЕРБЕЗПЕКИ**

**2017 Р.**

**Версія доповіді 1.0**

**31 грудня 2017 р.**

Посібник в рамках серії рекомендацій щодо викладання комп’ютерних наук

Спільна робоча група з питань освіти в галузі кібербезпеки

Асоціація обчислювальної техніки (Association for Computing Machinery, ACM)

Комп’ютерне товариство IEEE (IEEE Computer Society, IEEE-CS)

Спеціальна група з інформаційної безпеки та конфіденційності Асоціації інформаційних систем (Association for Information Systems Special Interest Group on Information Security and Privacy, AIS SIGSEC)

Технічний комітет з освіти в галузі інформаційної безпеки Міжнародної федерації по обробці інформації (International Federation for Information Processing Technical Committee on Information Security Education, IFIP WG 11.8)

Спільна робоча група (JTF) з питань CSEC2017

Діана Л. Берлі (Diana L. Burley), к.н. (співголова JTF, ACM)

Професор, Виконавчий директор з питань професійного та організаційного навчання, Інститут захисту інформаційної інфраструктури університету Джорджа Вашингтона, США

Метт Бішоп (Matt Bishop), к.н. (співголова JTF, ACM / IFIP)

Професор, Співдиректор факультету інформатики, Лабораторія комп’ютерної безпеки Каліфорнійського університету, Девіс, США

Скотт Бак (Scott Buck) (ACM)

Директор університетських програм Intel Labs, Intel, США

Джозеф Дж. Екстром (Joseph J. Ekstrom), к.н. (IEEE CS)

Почесний доцент, інформаційні технології, університет Бригама Янга, США

Лінн Фатчер (Lynn Futcher), к.н. (ACM / IFIP)

Доцент Університету Нельсона Мандели, Південна Африка

Девід Гібсон (David Gibson), к.н. (ACM)

Почесний професор, інформатика, факультет комп’ютерних та кібернетичних наук Академії військово-повітряних сил Сполучених Штатів Америки, США

Елізабет К. Хоторн (Elizabeth K. Hawthorne), к.н. (АСМ)

Старший професор, інформатика та кібербезпека, коледж округу Юніон, США

Сіддхарт Каза (Siddharth Kaza), к.н. (ACM)

Доцент кафедри комп’ютерних та інформаційних наук, факультет комп’ютерних та інформаційних наук університету Таусона, США

Яір Леві (Yair Levy), к.н. (AIS SIGSEC)

Професор, Директор з питань інформаційних систем і кібербезпеки, Центр захисту інформації, освіти і досліджень (CIPhER), Південно-Східний Університет Нова, США

Герберт Метторд (Herbert Mattord), к.н. (AIS SIGSEC)

Доцент, інформаційні системи, Директор з питань освіти, Інститут з навчання фахівців у галузі кібербезпеки, Державний університет Кеннесо, США

Аллен Перріш (Allen Parrish), к.н. (IEEE CS)

Професор, кібернетика, факультет кібернетики Військово-морської академії США, США

**ЗМІСТ**

Глава 1: Вступ до викладання кібербезпеки 9

1.1 Спільна робоча група 9

1.1.1 Концепція 10

1.1.2 Місія 10

1.1.3 Цілі 11

1.2 Цільова аудиторія 11

1.3 Джерела 12

1.4 Залучення світової спільноти 12

1.4.1 Міжнародні семінари 13

1.4.2 Глобальне опитування зацікавлених сторін 13

1.4.3 Подяка учасникам 14

1.5 Кібербезпека як дисципліна 14

1.6 Структура доповіді 15

Глава 2: Дисципліна «Кібербезпека» 16

2.1 Зростання кількості кіберзагроз 16

2.2 Виникнення кібербезпеки як дисципліни 17

2.3 Особливості програми з кібербезпеки 18

Глава 3: Структура навчальних планів з кібербезпеки 19

3.1 Філософія і підхід 19

3.2 Модель мислення 19

3.2.1 Галузі знань 20

3.2.2 Наскрізні концепції 21

3.2.3 Дисциплінарний підхід 22

Глава 4. Зміст навчального плану з кібербезпеки 23

4.1 Галузь знань: Захист даних 24

4.1.1 Розділи знань і теми 24

4.1.2 Основні поняття і цілі навчання 30

4.2 Галузь знань: Захист програмного забезпечення 31

4.2.1 Розділи знань і теми 31

4.2.2 Основні поняття і цілі навчання 36

4.3 Галузь знань: Захист компонентів 37

4.3.1 Розділи знань і теми 37

4.3.2 Основні поняття і цілі навчання 39

4.4 Галузь знань: Захист з’єднань 40

4.4.1 Розділи знань і теми 40

4.4.2 Основні поняття і цілі навчання 45

4.5 Галузь знань: Захист системи 47

4.5.1 Розділи знань і теми 47

4.5.2 Основні поняття і цілі навчання 50

4.6 Галузь знань: Захист людини 51

4.6.1 Розділи знань і теми 52

4.6.2 Основні поняття і цілі навчання 57

4.7 Галузь знань: Захист організації 58

4.7.1 Розділи знань і теми 59

4.7.2 Основні поняття і цілі навчання 68

4.8 Галузь знань: Захист суспільства 69

4.8.1 Розділи знань і теми 70

4.8.2 Основні поняття і цілі навчання 76

Глава 5: Галузеві перспективи кібербезпеки 78

5.1 Безліч техніко-ділових навичок 78

5.2 Кар’єрні можливості 79

5.3 Поєднання навчального плану з кібербезпеки з професійною практикою 80

5.3.1 Області застосування 80

5.3.2 Навчання та атестація 82

5.4 Основи підготовки фахівців 82

5.4.1 Реалізація «дорожньої карти» NCWF 83

5.4.2 Загальний огляд 85

5.4.3 Відповідні курси 85

5.4.4 Стратегії набуття KSA – знань, навичок і вмінь 85

5.4.5 Проблеми 86

Посилання

Додаток A: Учасники

Глобальна консультативна рада спільної робочої групи з питань освіти в галузі кібербезпеки

Галузева консультативна рада спільної робочої групи з питань освіти в галузі кібербезпеки

Робочі групи з галузей знань

Галузь знань: Захист даних

Галузь знань: Захист програмного забезпечення

Галузь знань: Захист компонентів

Галузь знань: Захист з’єднань

Галузь знань: Захист системи

Галузь знань: Захист людини

Галузь знань: Захист організації

Галузь знань: Захист суспільства

Рецензенти

Додаток B: Загальні таблиці основних понять 87

Додаток С: Зразки 88

Зразок навчального плану 88

Зразок плану підготовки фахівців 91

Зразок курсів 93

Таблиця рисунків

Рис. 1. Заходи щодо залучення світової спільноти 12

Рис. 2. Структура дисципліни «Кібербезпека» 18

Рис. 3. Модель мислення CSEC 19

Рис.4. Структура галузей знань 20

Рис. 5. Ув’язка моделі мислення CSEC і основного плану підготовки фахівців 83

Рис. 6. Елементи «дорожньої карти» для курсу 84

Рис. 7. Рецензенти відповідно до країн проживання

**Глава 1: Вступ до викладання кібербезпеки**

На загальну думку, по всьому світу наразі відчувається все більша нестача кваліфікованих фахівців і практиків в галузі кібербезпеки. І державні, і недержавні центри досліджень припускають, що до 2022 року налічуватиметься близько 1,8 млн. вакантних робочих місць в галузі кібербезпеки[[1]](#footnote-1). Попит на робочу силу є гострим, негайним і постійно зростаючим[[2]](#footnote-2). З метою підготовки необхідних фахівців, кафедри та факультети всіх комп’ютерних наук запускають ініціативи зі створення нових програм з кібербезпеки або введення спеціальних дисциплін у межах існуючих програм. Будь то розробка нових навчальних програм, чи введення нових предметів у межах існуючих програм, або розширення існуючого змісту курсу, ці навчальні заклади потребують рекомендацій щодо викладання такої дисципліни, заснованих на всебічному розумінні кібербезпеки, специфічних вимог до базової дисципліни, а також взаємозв’язку між навчальною програмою та планом підготовки фахівців з кібербезпеки.

У серпні 2015 р. Освітня рада Асоціації обчислювальної техніки (ACM) визнала нагальну потребу, що виникла, і вжила заходів, зібравши Спільну робочу групу з питань освіти в галузі кібербезпеки (CSEC2017) разом з іншими професійними та науковими товариствами і об’єднаннями фахівців з інформаційних технологій для розробки комплексних рекомендацій щодо освіти в галузі кібербезпеки.

Протягом майже п’яти десятиліть, починаючи з рекомендацій щодо викладання інформатики 1968 року[[3]](#footnote-3), освітня ініціатива ACM співпрацювала з іншими професійними та науковими товариствами з метою складання рекомендацій щодо розробки навчальних планів і програм з комп’ютерних наук. На сьогодні навчальні посібники ACM містять рекомендації щодо викладання таких дисциплін, як інформатика, обчислювальна техніка, інформаційні системи, інформаційні технології та програмна інженерія. Доповідь АСМ щодо Рекомендацій щодо викладання 2005 (CC2005), що в даний час оновлюється, надає огляд рекомендацій щодо викладання кожної з цих п’яти дисциплін[[4]](#footnote-4). Цей посібник CSEC2017 являє собою розширення освітньої ініціативи ACM з метою включення першої серії загальних рекомендацій щодо викладання кібербезпеки.

У зв’язку зі швидкою зміною природи і характеру кібербезпеки настійно рекомендується переглянути дані рекомендації щодо викладання протягом п’яти років з дати публікації.

**1.1 Спільна робоча група**

Спільна робоча група CSEC2017 з питань освіти в галузі кібербезпеки (JTF) була офіційно створена у вересні 2015 року в межах співпраці між основними міжнародними комп’ютерними об’єднаннями і товариствами: Асоціація обчислювальної техніки (ACM), Комп’ютерне товариство IEEE (IEEE-CS)[[5]](#footnote-5), Спеціальна група з інформаційної безпеки та конфіденційності Асоціації інформаційних систем (AIS SIGSEC)[[6]](#footnote-6) і Технічний комітет з освіти в галузі інформаційної безпеки Міжнародної федерації з обробки інформації (IFIP WG 11.8)[[7]](#footnote-7).

Освітня рада ACM призначила співголів JTF CSEC2017. Окрім призначених співголів до складу JTF CSEC2017 входять дев’ять провідних фахівців в галузі кібербезпеки, відібраних професійними товариствами для представлення зацікавлених сторін і надання різноманітних точок зору. Члени JTF перераховані на початку цього документа, де також зазначено до яких організацій і товариств вони належать.

JTF CSEC2017 є результатом проекту з кібер-освіти (CEP)[[8]](#footnote-8). Ініціатива CEP була організована в липні 2014 року групою фахівців в галузі інформатики, які представляли різні наукові установи та професійні товариства. Місія CEP була двоякою: ініціювати процеси для (1) розробки посібника з рекомендаціями щодо викладання у навчальних закладах і (2) створення основи для акредитації освітніх програм в області кібернаук.

Метою JTF CSEC2017 є просування першої місії СЕР:

*Розробка комплексних рекомендацій щодо викладання кібербезпеки, які сприятимуть розробці навчальних планів і відповідних освітніх програм на рівні післяшкільної освіти.*

Хоча JTF CSEC2017 вирішила використовувати загальноприйнятий термін «кібербезпека» замість терміну «кібернауки», висунутого СЕР, концептуально ці терміни узгоджуються.

**1.1.1 Концепція**

JTF CSEC2017 з самого початку її створення у вересні 2015 року активно працювала над визначенням параметрів проекту і формуванням основної концепції, місії і цілей. Концепція проекту:

*Навчальний посібник CSEC2017 стане основним джерелом комплексних рекомендацій щодо викладання кібербезпеки в навчальних закладах по всьому світу, які прагнуть розробити широкий спектр пропозицій щодо освіти в галузі кібербезпеки на рівні післяшкільної освіти.*

**1.1.2 Місія**

Місія CSEC2017 має на меті дві цілі:

* Розробити комплексні і гнучкі рекомендації щодо викладання кібербезпеки, які сприятимуть розробці навчальних планів і відповідних освітніх програм на рівні післяшкільної освіти;
* Підготувати навчальний посібник, який структурує дисципліну «Кібербезпека» і дає рекомендації навчальним закладам, які прагнуть розробити або змінити програми, спеціальні дисципліни та/або курси, а не директивний документ для підтримки одного типу програми.

**1.1.3 Цілі**

На основі вищезгаданої місії JTF CSEC2017 встановила наступні цілі, які необхідно досягти при створенні навчального посібника:

* Описати бачення спеціальних навиків з кібербезпеки;
* Визначити структуру дисципліни «Кібербезпека» шляхом розробки моделі мислення, яка визначає межі дисципліни і окреслює ключові аспекти структури навчального плану;
* Підтримувати актуальність навчальних програм і їхню відповідність потребам галузі кібербезпеки;
* Залучити якомога більше зацікавлених сторін шляхом безперервного залучення спільноти у процес розробки;
* Розробити рекомендації, які були б достатньо всеосяжними для підтримки різних типів програм;
* Розробити рекомендації, засновані на фундаментальних принципах, які забезпечують стабільність, але структуровані таким чином, щоб забезпечити гнучкість для підтримки мінливих потреб навчальних програм.

**1.2 Цільова аудиторія**

JTF CSEC2017 визначає первинну і вторинну цільові аудиторії для рекомендацій щодо викладання кібербезпеки.

Первинна аудиторія:

* Викладачі комп’ютерних дисциплін у навчальних закладах по всьому світу, зацікавлені в розробці програм з кібербезпеки, визначенні нових спеціальних дисциплін з кібербезпеки в рамках існуючих програм або розширенні існуючих програм (зокрема існуючі спеціальні дисципліни і курси) з метою включення предметів з кібербезпеки.

Вторинна аудиторія:

* Суб’єкти галузі, які допомагатимуть в розробці навчальних програм з кібербезпеки в ВНЗ, розроблятимуть галузеві програми і будуть роботодавцями випускників цих програм,
* Організатори тренінгів і програм підвищення кваліфікації;
* Викладачі дисциплін, не пов’язаних з комп’ютерними науками, які розробляють або мають намір розробляти суміжні програми, націлені на викладання концепцій кібербезпеки і освоєння необхідних навиків;
* Посадові особи навчальних закладів, до функцій яких входить нагляд за розробкою і переглядом програм і курсів;
* Розробники планів підготовки фахівців (державні і недержавні);
* Особи, що розробляють політику у даній галузі;
* Шкільні заклади, які готують учнів до отримання післяшкільної освіти в галузі кібербезпеки;
* Інші зацікавлені сторони, які беруть участь в ініціативах щодо підготовки фахівців з кібербезпеки.

**1.3 Джерела**

Рекомендації щодо викладання дисципліни, викладені в цьому документі, базуються на попередній роботі у сфері навчання і підготовки фахівців у галузях комп’ютерної безпеки, забезпечення інформаційної безпеки і кібербезпеки. Окрім джерел, перерахованих далі в цьому документі у розділі «Посилання», основними джерелами, що використовувалися при розробці цього документа, є:

* Навчальні плани з інформатики 2013: Рекомендації щодо викладання інформатики для програм бакалаврату (Computer Science Curricula 2013: Curriculum Guidelines for Undergraduate Degree Programs in Computer Science,),
* Міжнародна модель класифікації ІТ-навичок, необхідних для інформаційної ери (SFIA) (Global IT Skills Framework for the Information Age (SFIA)),
* Вимоги Агентства національної безпеки США і національних центрів передового досвіду Міністерства внутрішньої безпеки США у сфері кіберзахисту і кібероперацій (Requirements of the U.S. National Security Agency and U.S. Department of Homeland Security National Centers of Academic Excellence in Cyber Defense and Cyber Operations),
* Навчальні плани з інформаційних технологій 2017: Рекомендації щодо викладання інформаційних технологій для програм бакалаврату (Information Technology Curricula 2017: Curriculum Guidelines for Baccalaureate Degree Programs in Information Technology),
* Керівництво до зводу знань в області системної інженерії (Guide to the Systems Engineering Body of Knowledge),
* Національна ініціатива США з питань освіти в галузі кібербезпеки (NICE), основний план підготовки фахівців з кібербезпеки (U.S. National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework).

**1.4 Залучення світової спільноти**



Рис. 1. Заходи щодо залучення світової спільноти

JTF CSEC2017 постійно залучає широкі кола зацікавлених сторін до процесу розробки. Члени спільноти внесли свій внесок у формування підходу, змісту та організаційної структури посібника CSEC. Діяльність по залученню спільноти включала в себе: спеціальні сесії, панелі та семінари на конференціях за участю професійних об’єднань і товариств, міжнародні конференції, основні доповіді, вебінари, наради робочих груп, урядові брифінги та брифінги консультативної ради.

Як показано на рис. 1, заходи з залучення спільноти проводилися в різних регіонах світу. Ці заходи розглядалися в якості регіональних можливостей для збору інформації у широкого кола експертів з конкретних питань. Крім цих заходів, ключовими подіями у процесі розробки були проведення міжнародних семінарів та опитування зацікавлених сторін.

**1.4.1 Міжнародні семінари**

У 2016 році за підтримки корпорації Intel і Національного наукового Фонду США JTF організувала і провела Міжнародний семінар з питань освіти в галузі безпеки (ISEW), який відбувся 13-15 червня 2016 року в Філадельфії, штат Пенсільванія[[9]](#footnote-9). Семінар був організований для просування процесу розробки CSEC2017. В ході панельних дискусій та засідань робочих груп близько 75 зацікавлених сторін з міжнародної спільноти, що залучені до процесу освіти в галузі кібербезпеки, внесли свій внесок у зміст і структуру рекомендацій щодо навчальних планів, обговоривши два ключових питання:

* + Що повинно бути включено в навчальний план з кібербезпеки?
  + Як структурувати і поширити посібник з рекомендаціями щодо викладання дисципліни?

Повний звіт про засідання доступний на веб-сайті CSEC2017. Дані, зібрані за допомогою учасників ISEW, сприяли створенню першої версії моделі мислення CSEC2017 і послужили основою глобального опитування зацікавлених сторін.

У серпні 2016 року представники урядів 10 країн Асоціації держав Південно-Східної Азії (ASEAN) разом з лідерами Японії і Австралії взяли участь у брифінгу щодо проекту 2016 року, що проходив у Сінгапурі. У число представників ASEAN входили: Бруней, Малайзія, Лаос, Таїланд, Сінгапур, Камбоджа, М’янма, В’єтнам, Індонезія і Філіппіни.

Приблизно через рік після ISEW, 29-31 травня 2017 року JTF організувала сесію взаємодії зі спільнотою під час 10-ої Всесвітньої конференції з питань освіти в галузі інформаційної безпеки (WISE 10) в Римі, Італія. Учасники з таких країн, як Німеччина, Норвегія, Росія, Швеція, Південна Африка і Сполучені Штати, зібралися для обговорення проекту документа CSEC2017 V. 0.05 і для просування процесу його розробки. Доповідь про структуру та цілі семінару було опубліковано у протоколах WISE 10.

**1.4.2 Глобальне опитування зацікавлених сторін**

У вересні 2016 року, через рік після заходів з залучення спільноти і роботи з розробки документу, JTF запустила глобальне опитування зацікавлених сторін з метою отримання відгуків щодо пропонованої моделі мислення навчальних планів. Зацікавлених сторін було запрошено взяти участь в опитуванні шляхом направлення прямих запрошень, через оголошення на громадських освітніх і наукових форумах, соціальні мережі, тобто через веб-сайт JTF і LinkedIn, а також запрошення, надіслані через списки розсилки професійних асоціацій-учасників розробки рекомендацій. В ході опитування було отримано 231 відповідь від зацікавлених сторін, які проживають в 20 країнах та працюють в академічних колах, галузі та уряді і представляють всі п’ять комп’ютерні дисципліни.

Респонденти опитування запропонували JTF уточнити цільову аудиторію навчального посібника; уточнити визначення і розмежувати елементи моделі мислення навчального плану; надати додаткову інформацію про зміст кожної з галузей знань; спростити модель мислення; і адаптувати структуру для можливості розміщення нових тем. JTF використала ці зауваження для перегляду моделі мислення. Повний звіт щодо проведення опитування доступний на веб-сайті CSEC2017.

**1.4.3 Подяка учасникам**

JTF з вдячністю відзначає цінний внесок всіх учасників в наші зусилля по залученню спільноти. Ми особливо відзначаємо експертів з глобальних питань, які надають консультації, виступаючи в якості членів наших консультативних рад та робочих груп. Протягом усього процесу розробки цього документу члени Глобальної консультативної ради та Галузевої консультативної ради надавали консультації щодо процесу розробки, стратегій залучення міжнародної спільноти і конкретних питань змісту навчальних планів. Члени наших робочих груп по галузях знань надавали допомогу членам спільної робочої групи в питаннях розробки змісту навчальних планів за галузями знань.

Ми ретельно розглянули всі коментарі та критичні зауваження від членів спільноти; ми особливо вдячні за коментарі, надані в якості відгуків при проведенні опитування. Повний список учасників (включаючи учасників міжнародних семінарів), а також графічне представлення масштабів участі спільноти наводяться в додатку А в кінці цього документа[[10]](#footnote-10).

**1.5 Кібербезпека як дисципліна**

В Оглядовій доповіді CC2005 ACM визначає п’ять основних комп’ютерних дисциплін та визнає категорію комп’ютерних дисциплін, яка підкреслює зростаючу кількість змішаних або міждисциплінарних курсів.

* + Обчислювальна техніка,
  + Інформатика,
  + Інформаційні системи,
  + Інформаційні технології,
  + Програмна інженерія,
* Спеціальності зі змішаними дисциплінами (*xx Інформатика або Обчислювальні науки xx*).

JTF CSEC2017 просуває кібербезпеку як нову комп’ютерну дисципліну і позиціонує рекомендації щодо викладання кібербезпеки в контексті вищезазначених дисциплін. Ці п’ять дисциплін (перерахованих вище) часто служать основою нових навчальних програм з кібербезпеки (або навчальних курсів). В результаті дисциплінарний підхід формує рекомендації щодо глибини вивчення предмету і бажаних результатів навчання студентів. Спосіб, у який дисциплінарний підхід формує зміст рекомендацій, буде детально розглянуто у Главі 3 цього документа.

**1.6 Структура посібника**

Цей посібник, CSEC2017 V. 1.0, представляє напрацювання JTF. Посібник CSEC2017 містить огляд кібербезпеки як дисципліни з метою створення зразку навчального плану. У документі викладаються основні принципи і рекомендований зміст навчальних планів. Для надання більш широкого контексту, у посібнику висвітлюються галузеві перспективи кібербезпеки. Нарешті, з метою допомоги впровадженню викладеного, у посібнику розглядаються питання, пов’язані з освітньою практикою, пропонується алгоритм розробки «дорожніх карт», які пов’язують зразок навчального плану з планом підготовки фахівців, а також дається посилання на зразки курсу, навчального плану і плану підготовки фахівців, які показують, яким чином навчальні заклади можуть реалізовувати рекомендації.

«Дорожні карти» і приклади будуть постійно надходити через веб-сайт завдяки залученню спільноти: http://cybered.acm.org (найближчим часом почне працювати).

**Глава 2: Дисципліна «Кібербезпека»**

CSEC2017 JTF визначає кібербезпеку як:

*Заснована на обчисленнях дисципліна, що включає технології, фахівців, інформацію і процеси, покликані забезпечити роботу в умовах дій зловмисників. Кібербезпека включає в себе створення, експлуатацію, аналіз і тестування захищених комп’ютерних систем. Це міждисциплінарний курс, що включає аспекти права, політики, людські фактори, етику та управління ризиками.*

Кібербезпека – це заснована на обчисленнях дисципліна, що включає технології, фахівців, інформацію і процеси, покликані забезпечити роботу в умовах дій зловмисників. Вона спирається на основоположні області інформаційної безпеки і забезпечення цілісності і захисту інформації, при цьому фокусуючись на області комп’ютерної безпеки.

Потреба в кібербезпеці виникла при розробці перших мейнфреймів – універсальних ЕОМ. Для захисту цих пристроїв і обслуговуваних ними місій були впроваджені різні рівні безпеки. Зростаюча потреба у підтримці національної безпеки в кінцевому рахунку призвела до більш комплексних і технологічно складних засобів забезпечення безпеки. У перші роки кібербезпека, як вона застосовувалась, навіть якщо вона конкретно не визначалася як така, являла собою простий процес, що складався головним чином з забезпечення фізичної безпеки та класифікації документів. Основними загрозами безпеки були розкрадання обладнання, шпигунство з метою збору інформації про продукти систем і саботаж. У міру зростання залежності суспільства від широкої кібер-інфраструктури зростало і середовище виникнення загроз.

**2.1 Зростання кількості кіберзагроз**

У 1958 році було створено Агентство перспективних дослідницьких проектів при Міністерстві оборони США (ARPA), яке приступило до вивчення можливості створення надлишкової мережевої системи комунікацій для підтримки обміну комп’ютерними даними. В результаті наприкінці 1960-х років було створено мережу під назвою ARPANET, яку почали широко використовувати, що збільшувало можливості її використання зловмисниками.

Безпека, яка виходила за межі захисту фізичного місця розташування обчислювальних пристроїв, фактично почалася з однієї статті, опублікованій корпорацією RAND у лютому 1970 року для Міністерства оборони. У цій статті, RAND Report R-609, зроблено спробу визначити численні заходи контролю і механізми, необхідні для захисту комп’ютеризованої системи обробки даних.

У 1970-х роках розробка TCP (Transmission Control Protocol - протокол керування передачею) і IP (Internet Protocol - Інтернет протокол) призвела до появи Інтернету. Розвиток Всесвітньої павутини в 1980-х роках призвів до широкого використання Інтернету, що значно підвищило важливість кібербезпеки. Уряд США прийняв кілька ключових законодавчих актів, які офіційно закріпили визнання комп’ютерної безпеки в якості одного з найважливіших показників для федеральних інформаційних систем, зокрема такі акти, як закон 1986 року про комп’ютерне шахрайство та зловживання і закон 1987 року про комп’ютерну безпеку. Інтернет зрештою забезпечив повсюдне підключення практично до всіх комп’ютерів, при цьому цілісність і конфіденційність користувалися більш низьким пріоритетом, ніж доступність. Багато проблем, які вражають Інтернет сьогодні, є результатом браку усвідомлення важливості забезпечення безпеки в ті часи.

Ранні підходи до обчислень ґрунтувалися на засобах забезпечення безпеки, які застосовувалися у будівлях і приміщеннях розташування центрів обробки даних. У міру того, як застосування комп’ютерів, об’єднаних у мережу, при виконанні обчислень стало переважати, здатність фізично захистити комп’ютер, приєднаний до мережі, зникла, а інформація, що зберігалася, ставала більш вразливою для загроз безпеки. Великі організації почали включати засоби забезпечення безпеки в свої обчислювальні стратегії. Антивірусні продукти стали надзвичайно популярними, а кібербезпека з’явилася як самостійна дисципліна.

Завдяки Інтернету незахищені комп’ютерні мережі і мільярди підключених пристроїв знаходяться в безперервному зв’язку один з одним. Забезпечення безпеки інформації, що зберігається на кожному комп’ютері, залежить від обізнаності, навчання та застосування принципів кібербезпеки. Захист інформації, що зберігається на комп’ютері, може бути забезпечений шляхом попереднього визначення значущості інформації. Вибір засобів контролю безпеки і захисту інформації при її передачі, обробці та зберіганні повинен бути порівнянний зі значущістю інформації і середовищем загроз.

В останні роки зростає усвідомлення необхідності покращення забезпечення кібербезпеки, а також усвідомлення того, що кібербезпека важлива для національної оборони кожної країни. Зростаюча загроза кібератак змусила уряди і компанії краще усвідомити необхідність захисту комп’ютеризованих систем управління комунальними службами та іншою важливою інфраструктурою. Ще однією зростаючою проблемою є загроза втягнення національних держав у кібервійни і можливість того, що ділові та особисті інформаційні системи можуть стати об’єктами кібератак, якщо вони не будуть захищені.

**2.2 Виникнення кібербезпеки як дисципліни**

Враховуючи зростаючу залежність суспільства від глобальної комп’ютерної інфраструктури, не дивно, що кібербезпека стає самостійною дисципліною зі змістом, що охоплює багато інших підрозділів (наприклад, розробка програмного забезпечення, створення мереж, управління базами даних), які формують сучасну обчислювальну екосистему. В основі цього явища лежить необхідність підготовки фахівців, які виконуватимуть різні робочі функції для вирішення складних завдань, пов’язаних із забезпеченням безпеки функціонування системи, на базі цілісного підходу. Забезпечення безпеки функціонування включає в себе створення, експлуатацію, захист, аналіз і тестування захищених комп’ютерних систем.

Хоча кібербезпека є міждисциплінарним курсом, що включає аспекти права, політики, людські фактори, етику та управління ризиками, вона по своїй суті є дисципліною, заснованою на обчисленнях. Таким чином, як показано на рис. 2, навчальні програми в галузі кібербезпеки засновані на міждисциплінарному змісті і визначаються потребами і перспективами комп’ютерної дисципліни, які формують основу програми.



Рис. 2. Структура дисципліни «Кібербезпека»

|  |  |  |  |
| --- | --- | --- | --- |
| Human factors | Людські фактори | Computer science | Інформатика |
| Ethics | Етика | Computer engineering | Обчислювальна техніка |
| Law | Право | Information technology | Інформаційні технології |
| Policy | Політика | Information systems | Інформаційні системи |
| Risk management | Управління ризиками | Software engineering | Програмна інженерія |
| Interdisciplinary content | Міждисциплінарний зміст | Computing disciplines | Комп’ютерні дисципліни |
| Cybersecurity (a computing-based, inter-disciplinary course of study) | | Кібербезпека (міждисциплінарний курс, заснований на обчисленнях) | |

Кібербезпека як самостійна дисципліна все ще перебуває в зародковому стані. Враховуючи значні потреби в фахівцях, навчальні заклади розробляють ряд освітніх програм у цій галузі, в той час як інші коригують існуючі програми для включення кібербезпеки. Рекомендації щодо викладання кібербезпеки, представлені в цьому документі, складені на основі комп’ютерних дисциплін: інформатика, обчислювальна техніка, інформаційні технології, інформаційні системи та програмна інженерія.

**2.3 Особливості програми з кібербезпеки**

Кожен випускник за спеціальністю «Кібербезпека» повинен завершити програму з кібербезпеки, яка включає:

* Основи комп’ютерних дисциплін (наприклад, інформатика, інформаційні технології);
* Наскрізні концепції, які широко застосовуються у всіх спеціалізаціях в галузі кібербезпеки (наприклад, властивий кібербезпеці змагальний характер мислення);
* Сукупність знань, що містять необхідні знання та навички в галузі кібербезпеки;
* Пряме відношення до ряду спеціалізацій, що відповідають сферам діяльності, які користуються попитом;
* Приділення особливої уваги етичній поведінці і професійним обов’язкам, пов’язаним з діяльністю в галузі.

Рекомендації щодо викладання, зібрані в цьому документі, допоможуть навчальним закладам розробити програми з кібербезпеки, які відповідають кожному з цих критеріїв.

**Глава 3: Структура навчальних планів з кібербезпеки**

Для отримання кваліфікації в цій галузі, програми з кібербезпеки повинні включати:

* Теоретичні і концептуальні знання, необхідні для розуміння дисципліни і
* Можливості для розвитку практичних навичок, що сприяють застосуванню цих знань.

Знання і матеріали, включені в будь-яку програму з кібербезпеки, вимагають тонкого балансу широти і глибини охоплення, а також відповідності потребам у фахівцях. Також необхідна структура, яка одночасно забезпечує узгодженість програм аналогічних типів і гнучкість, обумовлені як потребами, так і досягненнями в галузі знань. Рекомендації щодо викладання дисципліни, представлені в цій главі, підтримують і врівноважують досягнення цих цілей.

**3.1 Філософія і підхід**

Модель мислення CSEC (далі - модель мислення) заснована на ретельному вивченні існуючих навчальних програм у галузі наукової освіти, комп’ютерної освіти і освіти в галузі кібербезпеки. Наша філософія, яка частково сформована науковими стандартами наступного покоління Національної дослідницької ради США[[11]](#footnote-11), розглядає кібербезпеку як сукупність знань, заснованих на міцних засадах, які постійно розширюються, уточнюються і переглядаються за допомогою практики, заснованої на фактичних даних.

**3.2 Модель мислення**

Модель мислення, зображена на рис. 3, має три виміри: галузі знань, наскрізні концепції та дисциплінарні підходи.

Хоча в явному вигляді цей аспект моделі не визначено, основоположні вимоги лежать в основі і підтримують весь зміст навчальних програм. Ці вимоги включають такі компетенції, як комунікація, математична грамотність, аналітичні навички та навички вирішення проблем, критичне мислення і командна робота, які розвиваються завдяки загальній освіті. Разом з технічною грамотністю і етичною поведінкою, ці вимоги допомагають студентам стати корисними членами суспільства.



Рис. 3 Модель мислення CSEC

|  |  |  |  |
| --- | --- | --- | --- |
| Disciplinary lenses | Дисциплінарні підходи | Connection | З’єднання |
| Information technology | Інформаційні технології | Human | Людина |
| Information systems | Інформаційні системи | Organization | Організація |
| Computer science | Інформатика | Societal | Суспільство |
| Computer engineering | Обчислювальна техніка | Cross-cutting concepts | Наскрізні концепції |
| Software engineering | Програмна інженерія | Confidentiality | Конфіденційність |
| Other disciplines | Інші дисципліни | Integrity | Цілісність |
| Body of knowledge | Сукупність знань | Availability | Доступність |
| 8 knowledge areas | 8 галузей знань | Risk | Ризик |
| Data | Дані | Adversarial thinking | Змагальний характер мислення |
| Software | Програмне забезпечення | Systems thinking | Системне мислення |
| Component | Компонент |  |  |

**3.2.1 Галузі знань**

Галузі знань (KA) служать базовою організаційною структурою змісту програми з кібербезпеки. Кожна галузь знань складається з критично важливих знань, що мають велике значення в межах різних комп’ютерних дисциплін. Галузі знань структуровані як гнучкі області моделі мислення, щоб забезпечити можливість розширення або стиснення матеріалу за потреби. У сукупності галузі знань являють собою всю сукупність знань в галузі кібербезпеки.

**Основні поняття кібербезпеки.** Основні поняття кожної галузі знань відображають навички з кібербезпеки, якими повинен оволодіти кожен студент, незалежно від спеціалізації програми. Основні поняття кібербезпеки необхідно викладати на ранньому етапі навчання і потім зміцнювати їх в рамках кожної програми з кібербезпеки.

Розділи знань (KU) являють собою тематичні групи, які охоплюють кілька суміжних тем; теми охоплюють необхідний матеріал навчальних планів для кожного KU. Результати навчання - це опис того, що студенти повинні знати або вміти робити. Як показано на рисунку 4, KA можуть містити кілька розділів знань, тем і результатів навчання. Конкретні результати навчання за темами, які містяться у кожному КА, наведені в прикладах.

*Основні поняття чітко визначені в кожній галузі знань. Ці поняття можуть відображатися як конкретні розділи знань, як теми в межах розділів знань або як сукупності тем у межах розділів знань. У сукупності основні поняття з усіх галузей знань повинні охоплюватися в кожній програмі з кібербезпеки. Конкретні результати навчання за основним поняттями включені в навчальний план, описаний у главі 4*.



Рис. 4 Структура галузей знань

|  |  |
| --- | --- |
| Knowledge area | Галузь знань |
| Knowledge unit | Розділ знань |
| Topic | Тема |
| Learning outcomes | Цілі навчання |
| Content influenced by disciplinary lens and institution type | Знання, на які впливають дисциплінарні підходи і тип закладу |

У моделі мислення кожний розділ знань відповідає наступним критеріям:

* Має широке (хоча і змінне, засноване на дисциплінарному підході) значення в декількох комп’ютерних дисциплінах;
* Надає ключовий інструмент для розуміння або дослідження складних понять кібербезпеки,
* Є таким, що можна пояснити і вивчити з часом і з підвищенням рівня глибини вивчення і складності.

Хоча основна увага в кожній галузі знань приділяється розробці, захисту та підтриманню параметрів безпеки, деякі програми можуть включати вивчення інструментів і методів обходу механізмів захисту, таких як курс тестування на можливість проникнення. Через змагальний характер кібербезпеки вивчення атакуючих або хакерських методів часто є хорошим способом розвинути навички з забезпечення захисту. Всі галузі знань включають в себе розділи знань, які можна розглядати як з точки зору кібер-захисту, так і з точки зору кібер-злочинів.

Галузі знань не є взаємовиключними, тому деякі розділи знань можуть відноситися і можуть бути логічно віднесені до декількох галузей знань. У той час як рекомендації щодо викладання різних дисциплін будуть відрізнятися, розділи знань навмисно повторюються в декількох галузях знань (з перехресними посиланнями). Оскільки розділи знань не обов’язково відповідають курсам або блокам курсу, курси з кібербезпеки зазвичай містять теми з декількох розділів знань. Тому розміщення розділу знань в одній галузі знань не повинно виключати його охоплення в інших галузях знань.

**3.2.2 Наскрізні концепції**

Наскрізні концепції допомагають студентам досліджувати зв’язки між різними галузями знань і мають основоположне значення для здатності людини розуміти галузь знань незалежно від дисциплінарного підходу. Такі концепції «забезпечують організаційну схему взаємодії знань»[[12]](#footnote-12) в цілісному уявленні кібербезпеки. Наскрізні концепції також посилюють спосіб мислення з точки зору безпеки, що забезпечується кожною галуззю знань.

Модель мислення включає в себе наступні шість наскрізних концепцій:

* **Конфіденційність**. Правила, що обмежують доступ до системних даних та інформації колом уповноважених осіб.
* **Цілісність.** Забезпечення точності та достовірності даних та інформації.
* **Доступність.** Дані, інформація і система доступні.
* **Ризик.** Потенційний прибуток або збиток.
* **Змагальний характер мислення**. Процес мислення, який розглядає потенційні дії супротивника, націлені на перешкоджання досягнення бажаного результату.
* **Системне мислення**. Процес мислення, який розглядає взаємодію між соціальними і технічними обмеженнями для забезпечення функціонування.

**3.2.3 Дисциплінарний підхід**

Дисциплінарний підхід - це третій вимір моделі мислення. Являє собою базову обчислювальну дисципліну, на основі якої може бути розроблена програма з кібербезпеки. Дисциплінарний підхід визначає підхід, глибину знань і цілі навчання, отримані у результаті взаємодії тем, основних та наскрізних концепцій. Модель мислення охоплює сучасні комп’ютерні дисципліни, визначені ACM: інформатика, обчислювальна техніка, інформаційні системи, інформаційні технології та програмна інженерія.

Застосування наскрізних концепції та/або рівень глибини знань, що даються в рамках кожного розділу знань, можуть відрізнятися в залежності від дисциплінарного підходу. Наприклад, охоплення поняття «ризик» у контексті захисту даних може відрізнятися для студентів програми з кібербезпеки інформатики і програми з кібербезпеки інформаційних систем. Приклади ілюструють цю взаємодію.

**Глава 4. Зміст навчального плану з кібербезпеки**

Зміст навчального плану було складено і зведено воєдино з різних джерел (перераховані у вільному порядку): ACM/IEEE CS2013; ACM/IEEE IT2017; центри академічної науки (САЕ) Агентство національної безпеки США та Департамент внутрішньої безпеки; (ISC)2; документи з основним планом підготовки фахівців, таких як Основний план підготовки фахівців з кібербезпеки, розроблені Національною ініціативою США з питань освіти в галузі кібербезпеки (NCWF); Основні ІТ-навички, необхідні в інформаційну епоху (SFIA); практичний курс за підтримки університету офісних програм Intel; Національний науковий фонд США; Центр урядового зв’язку Великобританії (GCHQ); робочі групи, створені фахівцями галузі; інші джерела, надані співтовариством зацікавлених сторін.

Розділи цієї глави містять огляд змісту навчальних планів з кожної галузі знань. У таблиці для кожної галузі знань перераховані основні поняття, розділи знань і теми з кожній галузі знань. У багатьох випадках були включені конкретні рекомендації щодо висвітлення певних тем. Для уточнення розділів знань і тем, JTF скликала експертів з метою створення робочих груп у кожній галузі знань (KAWG). Члени KAWG вказані за галузями знань в додатку A.

Як зазначено вище, основні поняття у галузях знань відображають професійні навички з кібербезпеки, якими повинен оволодіти кожен студент, незалежно від спрямованості програми. Основні поняття зазначаються в кожному розділі галузей знань і представлені разом у додатку В.

**Примітка:** деякі розділи знань і теми в галузях знань здаються зайвими. Такі розділи знань та теми вказані навмисно з метою забезпечення охоплення специфічного матеріалу в кожній конкретній галузі знань і наголошення важливості цих основних розділів знань і тем у всій сукупності знань з кібербезпеки.

У таблицях з кожної галузі знань містяться перехресні посилання на інші таблиці з галузей знань, що містять важливу додаткову інформацію. Перехресні посилання знаходяться у лівій колонці під заголовком «Розділи знань», виділені курсивом і вказані у квадратних дужках [ ].

Див. додаток C для огляду практичних прикладів, що показують галузі знань і розділи знань у різних видах програм. Приклади навчальних планів демонструють, як навчальні плани конкретних закладів охоплюють основні поняття галузі знань і деякі підмножини розділів знань. Приклади представлені на веб-сайті завдяки залученню спільноти (http://cybered.acm.org/) з метою показати, як зміст навчального плану з кібербезпеки може бути організований різними способами.

У таблицях наведено рекомендації для розробників навчального плану або курсу. Такі розробники повинні ілюструвати конкретними прикладами теми, які охоплюються їхнім курсом. Наприклад, опис/рекомендації з викладання теми «Логічний контроль доступу до даних» розділу знань «Керування доступом» галузі знань «Захист даних» перераховує кілька типів контролю, включаючи списки осіб з повноваженнями по доступу, повноважне керування доступом тощо. Групи, що спеціалізуються на безпеці мобільних пристроїв, матимуть у навчальному плані заняття з керування доступом для Android, навіть якщо такі заняття не зазначені в стовпці Опис/Рекомендації щодо викладання. Система Android не надає контроль доступом на основі атрибутів на час написання цього документа; тому навчальний план для груп за такою спеціальністю не містить занять з такою темою. Аналогічним чином, навчальний план з сучасної криптографії буде включати «Режими роботи для блокових шифрів» (обговорення/рекомендації щодо викладання теми «Симетричні шифри (з закритим ключем)» розділу знань «Криптографія» галузі знань «Захист даних»), такі як GCM, хоча в обговоренні/рекомендаціях щодо викладання явно не згадується цей режим. Ці два приклади підкреслюють, що рекомендації щодо викладання дисципліни містять теми, які не обов’язкові для включення в навчальний план. Конкретний зміст цих тем залишено на розсуд розробника навчального плану, тому що тільки ця особа знає цілі групи і потреби студентів, і тому може визначити, як необхідно розкрити кожну тему для задоволення цих цілей і потреб.

**4.1 Галузь знань: Захист даних**

Галузь знань з захисту даних фокусується на захисті даних при зберіганні, під час обробки і передачі. Ця галузь знань вимагає застосування математичних та аналітичних алгоритмів в повному обсязі.

**4.1.1 Розділи знань і теми**

У наступній таблиці перераховані основні поняття, розділи знань і теми галузі знань з захисту даних.

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ ДАНИХ** | | |
| **Основні поняття**  - Основні концепції криптографії,  - Цифрова криміналістика,  - Наскрізний захищений зв’язок,  - Цілісність і автентифікація даних,  - Безпека зберігання інформації. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Криптографія |  |  |
|  | Основні концепції | У цій темі розглядаються основні концепції і поняття, що закладають основу для вивчення інших матеріалів розділу знань. Ця тема включає наступне:   * Шифрування/дешифрування, автентифікація відправника, цілісність даних, неможливість відмови від авторства, * Класифікація атак (за наявності тільки шифрованого тексту, відомого відкритого тексту, обраного відкритого тексту, з вибором шифрованого тексту), * Криптографія з закритим ключем (симетрична) та криптографія з відкритим ключем (асиметрична), * Теоретико-інформаційний підхід (одноразовий ключ, * теорема Шеннона), * Розрахункова стійкість. |
|  | Поглиблені концепції | Ця тема містить наступне:   * Розширені протоколи: * докази з нульовим розголошенням та протоколи, * поділ секретної інформації, * блокування, * неочевидний обмін інформацією, * протокол конфіденційного обчислення, * Передові розробки: повністю гомоморфне шифрування, обфускація, квантова криптографія та схема KLJN. |
|  | Математична підготовка | Ця тема має важливе значення для розуміння алгоритмів шифрування. У разі потреби можна включити більш поглиблені концепції. Ця тема включає наступне:   * Числова система залишків, * Теореми Ферми, Ейлера, * Первісні корені, задачі дискретного логарифмування, * Тест простоти, розкладання великих чисел, * Еліптичні криві, решітки та складні ґратчасті задачі, * Абстрактна алгебра, кінцеві поля, * Теорія інформації. |
|  | Шифри в історії | Ця тема включає в себе інформацію про наступні шифри і їхнє поточне застосування (якщо таке є):   * Шифр зсуву, аффінний шифр, шифр заміщенням, шифр Віженера, ROT-13, * Шифр Гілла, машина Енігма та інші. |
|  | Симетричні шифри (з закритим ключем) | Ця тема включає наступне:   * Блочні шифри B і потокові шифри (псевдовипадкові перестановки, псевдовипадкові генератори), * Мережа Фейстеля, стандарт шифрування даних (DES), * Розширений стандарт шифрування (AES), * Режими роботи блочних шифрів, * Диференціальна атака, лінійна атака, * Потокові шифри, регістри зсуву з лінійним зворотним зв’язком, RC4. |
|  | Асиметричні шифри (з відкритим ключем) | Ця тема включає наступне:   * Теоретичні концепції (обчислювальна складність, одностороння функція з секретом), * Простий алгоритм RSA, * Слабкі місця простого алгоритму RSA, доповнений алгоритм RSA, * Протокол Діффі-Геллмана, * Шифр Ель-Гамаля, * Інші шифри з відкритим ключем, включаючи Гольдвассер-Мікалі, Рабіна, Пейє (Paillier), Мак Еліса, * Шифри на основі еліптичних кривих. |
| Цифрова криміналістика  [*Див. для отримання додаткової інформації також галузь знань «Захист системи», стор. 39*] |  |  |
|  | Введення | Ця тема включає наступне:   * Визначення, * Обмеження і типи інструментів (відкритий вихідний код проти закритого вихідного коду) |
|  | Правові аспекти | Ця тема включає наступне:   * Право на недоторканність приватного життя, * Четверта і п’ята поправки, * Захист ключів шифрування у відповідності з п’ятою поправкою, * Види правових підстав (згода власника, ордер на обшук, FISA - закон про негласне спостереження за агентами іноземних розвідок, розділ III (прослуховування), відмова від права, невідкладні обставини, знаходитись у всіх на виду тощо), * Захист від судових процесів (наприклад, інформація про абонента інтернет-провайдера через повістку до суду, транзакційні дані сервера електронної пошти з судового наказу 2703(d), повний контент через ордер на обшук тощо), * Запит на збереження цифрових доказів (наприклад, через лист про збереження 2703(f)), * Письмові показання під присягою, показання та свідчення |
|  | Цифрові криміналістичні інструменти | Ця тема включає наступне:   * Типи, * Артефакт-орієнтовані проти універсальних інструментів, * Вимоги, * Обмеження. |
|  | Розслідування | Ця тема включає наступне:   * Попередження, * Виявлення доказів, * Збір і збереження доказів, * Строки, звітність, порядок передачі і зберігання доказів, * Достовірність доказів |
|  | Отримання і збереження доказів | Ця тема включає наступне:   * «Витягнути штепсельну вилку» проти пріоритизації, * Блокування запису, * Криміналістично підготовлені носії інформації, * Створення образу, * Отримання мінливих доказів, * Криміналістична експертиза працюючої системи/комп’ютера, * Порядок передачі і зберігання доказів |
|  | Аналіз доказів | У цій темі розглядаються знання (обізнаність про існування продукту), атрибути (компоненти та можливі модифікації продукту), походження/причина (чому продукт існує), ймовірність виявлення (як інструменти визначають місце знаходження/ розглядають продукт), актуальність (значимість у контексті конкретного розслідування).  Включає наступне:   * Джерела цифрових доказів, * Видалені і відновлені файли, тимчасові файли, * Метадані, * Файли диспетчера черги друку, * Вільний простір, * Файли сплячого режиму, * Реєстр Windows, * Історія браузерів, * Файли журналів, * Файлова система, * Відновлення файлів і * Виділення однорідних масивів даних для відновлення видалених файлів (File carving) |
|  | Представлення результатів | Ця тема включає наступне:   * Аналіз часової шкали, * Атрибуція, * Непрофесійні проти технічних пояснень, * Аналітична записка, * Детальні звіти і * Обмеження |
|  | Достовірність доказів | Ця тема включає наступне:   * Алгоритми хешування (MD5, SHA-1 та ін.), * Хешування всього носія проти окремих файлів, * Хешування перед і після перевірки |
|  | Звітність, реагування і врегулювання інцидентів | Ця тема включає наступне:   * Структура звіту, * Виявлення і аналіз інцидентів, * Локалізація, ліквідація та відновлення, * Заходи після інцидентів, * Обмін інформацією |
|  | Криміналістичне дослідження мобільних пристроїв | Ця тема включає наступне:   * Бездротові технології, * Технологія мобільного зв’язку, * Збір / ізоляція мобільних пристроїв, * Мобільні операційні системи (ОС) і додатки, * Мобільні продукти |
| Цілісність і автентифікація даних | Складність автентифікації | Ця тема включає наступне:   * Багатофакторна автентифікація, * Криптографічні токени, * Криптографічні пристрої, * Біометрична автентифікація, * Одноразові паролі, * Автентифікація на основі знань. |
|  | Методи злому пароля | Ця тема включає наступне:   * Перебір за словником, * Атака методом грубої сили, * Райдужна таблиця , * Фішинг і соціальна інженерія, * Атака за допомогою шкідливих програм, * «Павучковий» метод (Spidering), * Автономний аналіз, * Інструменти для злому паролів |
|  | Методи зберігання пароля | Ця тема включає наступне:   * Криптографічні хеш-функції SHA-256, SHA-3, стійкість до колізій), * Сіль (модифікатор), * Кількість ітерацій, * Формування ключа на основі пароля |
|  | Цілісність даних | Ця тема включає наступне:   * Коди автентифікації повідомлення (HMAC, CBC-MAC), * Цифровий підпис, * Автентифіковане шифрування, * Хеш-дерева. |
| Керування доступом |  |  |
|  | Фізичний захист даних | Ця тема включає наступне:   * Захист центру обробки і зберігання даних, включаючи доступ з ключем, кабіну-пастку, ключ-карти і відеоспостереження, * Захист на рівні серверної стійки (Rack-level security), * Знищення даних |
|  | Логічний контроль доступу до даних | Ця тема включає наступне:   * Списки керування доступом, групові політики, паролі, * Дискреційне керування доступом (DAC), * Мандатне керування доступом (MAC), * Керування доступом на основі ролей (RBAC), * Керування доступом на основі атрибутів (ABAC), * Керування доступом на основі правил (RAC), * Керування доступом на основі історії (HBAC), * Керування доступом на основі ідентифікаційної інформації (IBAC), * Керування доступом на основі організації (OrBAC), * Федеративні посвідчення та керування доступом |
|  | Проектування архітектури системи безпеки | Ця тема включає наступне:   * Принципи архітектури системи безпеки, * Захист інформації в комп’ютерних системах |
|  | Методи запобігання витоку даних | Ця тема включає наступне:   * Контроль за дозволеними межами, * Канали, * Адресати, * Методи обміну даними. |
| Протоколи захищеного зв’язку | Протоколи прикладного та транспортного рівнів | Ця тема включає наступне:   * HTTP, * HTTPS, * SSH, * SSL / TLS. |
|  | Атаки на рівні TLS | Ця тема включає наступне:   * Атака типу Downgrade, * Підробка сертифікатів, * Наслідки крадіжки кореневих сертифікатів, * Прозорість сертифіката |
|  | Міжмережевий/ мережевий рівні | Ця тема включає IPsec і VPN. |
|  | Протоколи збереження конфіденційності | Ця тема включає Mixnet, Tor, протокол шифрування повідомлень Off-the-record і Signal. |
|  | Канальний рівень | Ця тема включає L2TP, PPP і RADIUS |
| Криптоаналіз |  |  |
|  | Класичні атаки | Ця тема включає наступне:   * Атака методом грубої сили, * Атаки на основі частотного аналізу, * Атаки на машину Енігма, * Атака «днів народження» |
|  | Атаки сторонніми каналами | Ця тема включає наступне:   * Атаки по часу, * Атаки по енергоспоживанню, * Метод диференціальних спотворень |
|  | Атаки на шифри з закритим ключем | Ця тема включає наступне:   * Диференціальна атака, * Лінійна атака, * «Зустріч посередині» (Meet-in-the-middle attack) |
|  | Атаки на шифри з відкритим ключем | Ця тема включає в себе алгоритми факторингу (методи Полларда p-1 і rho, методи квадратичного решета і решета числового поля). |
|  | Алгоритми для вирішення задач дискретного логарифмування | Ця тема включає наступне:   * Алгоритм Поліга-Геллманна, * Алгоритм великих і малих кроків, * Метод Полларда rho |
|  | Атаки на RSA | Ця тема включає наступне:   * Спільно використовуваний секретний модуль, * Малі значення відкритої експоненти, * Частково відома експонента (Partially exposed prime factors) |
| Конфіденційність даних  [*Див. для отримання додаткової інформації також «Захист людини», стор 44, «Захист організації», стор 51 і «Захист суспільства», стор 62*] |  |  |
|  | Огляд | Ця тема включає наступне:   * Визначення понять (Брандіс, Солове), * Правові аспекти (HIPAA, FERPA, GLBA), * Збір даних, * Агрегування даних, * Поширення даних, * Вторгнення в приватне життя, * Соціальна інженерія, * Соціальні мережі |
| Захист сховищ інформації |  |  |
|  | Шифрування диску і файлів | Ця тема містить порівняння шифрування апаратного і програмного забезпечення. |
|  | Видалення даних | Ця тема включає наступне:   * Перезапис, розмагнічування, * Методи фізичного знищення, * Залишкова пам’ять |
|  | Маскування даних | Ця тема включає в себе потреби і методи  маскування даних. Нижче наведено неповний список  підтем, які слід розглянути:   * Маскування даних для тестування, * Маскування даних для обфускації, * Маскування даних для конфіденційності. |
|  | Захист бази даних | Ця тема включає наступне:   * Доступ / автентифікація, ревізія, * Парадигми інтеграції додатків. |
|  | Законодавчі акти в сфері захисту даних | У цій темі розглядаються правові аспекти захисту даних,  Законодавчі акти і політика, що регулюють захист даних (наприклад, HIPAA). У ній також міститься введення в інші правові теми в галузі знань «Захист організації» |

**4.1.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Основні поняття криптографії |  |
|  | Опишіть призначення криптографії і перелічіть способи її використання при передачі даних. |
|  | Дайте визначення наступним термінам: шифр, криптоаналіз, алгоритм шифрування, криптологія; опишіть два основних методи (шифри) для перетворення відкритого тексту в шифротекст. |
|  | Поясніть, як інфраструктура відкритих ключів підтримує цифровий підпис і шифрування; обговоріть обмеження та вразливості. |
|  | Обговоріть небезпеки винаходу власних криптографічних методів. |
|  | Опишіть, які криптографічні протоколи, інструменти і методи підходять для даної ситуації. |
| Наскрізний захищений зв’язок  [*Див. для отримання додаткової інформації також галузь знань «Захист з’єднань», стор. 32*] |  |
|  | Поясніть цілі наскрізного захисту даних. |
| Цифрова криміналістика |  |
|  | Опишіть, що таке цифрове розслідування, джерела цифрових доказів і обмеження криміналістичної експертизи. |
|  | Порівняйте і зіставте різноманітність інструментів криміналістичної експертизи. |
| Цілісність даних і автентифікація |  |
|  | Поясніть концепції автентифікації, авторизації, керування доступом та цілісності даних. |
|  | Поясніть різні методи автентифікації та їх сильні і слабкі сторони. |
|  | Поясніть різні можливі атаки на паролі. |
| Видалення даних |  |
|  | Опишіть різні методи видалення даних |

**4.2 Галузь знань: Захист програмного забезпечення**

Галузь знань з захисту програмного забезпечення зосереджена на розробці і використанні програмного забезпечення, яке надійно зберігає параметри безпеки інформації і систем, які воно захищає. Захист системи, а також даних, які вона зберігає і якими управляє, в значній мірі залежить від захисту її програмного забезпечення. Захист програмного забезпечення залежить від того, в якій мірі вимоги відповідають потребам, які програмне забезпечення повинно вирішувати, наскільки якісно програмне забезпечення розроблено, впроваджено, протестовано, розгорнуто і підтримується. Документація має вирішальне значення для того, щоб зрозуміти ці міркування, а етичні міркування виникають впродовж процесів створення, впровадження, використання і вилучення з експлуатації програмного забезпечення.

Галузь знань з захисту програмного забезпечення вирішує ці проблеми безпеки. Розділи знань у цій галузі знань складаються з фундаментальних принципів і практики.

**4.2.1 Розділи знань і теми**

У нижченаведеній таблиці представлені основні принципи, поняття, розділи знань і теми галузі знань з захисту програмного забезпечення. Ці розділи знань були перевірені робочою групою з захисту програмного забезпечення з використанням переліку Топ 10 вразливостей від Відкритого проекту з забезпечення безпеки веб-додатків (Open Web Application Security Project - OWASP) і «Уникнення топ-10 недоліків проектування системи захисту програмного забезпечення» від IEEE

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ** | | |
| **Основні поняття**  - Фундаментальні принципи проектування, включаючи принципи мінімальних привілеїв, відкритого проектування і «абстрактної фабрики»,  - Вимоги безпеки та їх роль в проектуванні,  - Проблеми реалізації,  - Статичне та динамічне тестування,  - Налаштування конфігурації і виправлення,  - Етика, особливо при розробці, тестуванні та розкритті вразливостей. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Фундаментальні принципи  [*Див. для отримання додаткової інформації також галузь знань «Захист компонентів», стор. 29*] |  | Цей розділ знань містить принципи, що лежать в основі як проектування, так і реалізації. Перші п’ять - це принципи обмежувань, наступні три - принципи простоти, а решта - методологічні принципи. |
|  | Принцип мінімальних привілеїв | Програмне забезпечення повинно мати тільки ті привілеї, які необхідні для виконання завдання. |
|  | Принцип відмовостійких значень за замовчуванням | Початковий стан має містити заборону на доступ, якщо доступ явно не потрібен. Якщо програмному забезпеченню не надано явний доступ до об’єкта, йому має бути відмовлено в доступі до цього об’єкту, і стан захисту системи повинен залишатися незмінним. |
|  | Принцип перевірки кожного дозволу на доступ (complete mediation) | Програмне забезпечення має перевіряти кожен доступ до об’єктів, щоб гарантувати, що доступ дозволено. |
|  | Принцип поділу повноважень | Програмне забезпечення не має надавати доступ до ресурсу або вчиняти дії, пов’язані з безпекою, на основі однієї умови. |
|  | Принцип мінімізації довіри | Програмне забезпечення має перевіряти всі вхідні дані і результати всіх дій, пов’язаних з безпекою. |
|  | Принцип спрощення механізму захисту | Засоби захисту програмного забезпечення повинні бути максимально простими. |
|  | Принцип мінімізації загального механізму | Спільне використання ресурсів повинно бути максимально зменшене. |
|  | Принцип найменшого подиву | Засоби захисту програмного забезпечення та механізми безпеки, що застосовуються ним, повинні бути спроектовані таким чином, щоб їх робота була логічною і максимально простою. |
|  | Принцип відкритого проектування | Безпека програмного забезпечення і того, що воно забезпечує, не повинна залежати від секретності його проектування або реалізації. |
|  | Принцип багаторівневості | Розробка програмного забезпечення рівнями так, щоб модулі даного рівня взаємодіяли тільки з модулями на рівень вище або нижче. Це дозволяє тестувати програмне забезпечення на одному рівні, використовуючи методи тестування «зверху вниз» або «знизу вгору», а також зменшує кількість точок доступу, забезпечуючи дотримання принципу поділу повноважень. |
|  | Принцип «абстрактної фабрики» | Приховує внутрішні елементи кожного рівня, роблячи доступними тільки інтерфейси; це дозволяє змінювати спосіб виконання завдань на рівні, не зачіпаючи компоненти інших рівнів. |
|  | Принцип модульності | Проектуйте і реалізуйте програмне забезпечення як набір взаємодіючих компонентів (модулів); насправді кожен інтерфейс модуля є абстракція. |
|  | Принцип повного зв’язку | Зв’яжіть проектування системи захисту програмного забезпечення і реалізацію з вимогами до системи захисту такого програмного забезпечення. |
|  | Принцип проектування ітераціями | Плануйте проектування таким чином, щоб у разы потреби можна було вносити зміни. Це зменшує вплив на безпеку зміни дизайну, якщо специфікації не відповідають середовищу, в якому використовується програмне забезпечення. |
| Проектування |  | У цьому розділі знань описуються методи включення міркувань безпеки при розробці програмного забезпечення. |
|  | Визначення вимог безпеки | Починаючи з бізнес-завдань, місії або інших цілей, також визначте, які вимоги безпеки необхідні для успішної реалізації. Вони також можуть бути визначені або змінені у міру розробки програмного забезпечення. |
|  | Специфікація вимог безпеки | Переведіть вимоги безпеки в таку форму, якою можна користуватися (формальні специфікації, неформальні специфікації, специфікації для тестування). |
|  | Життєвий цикл розробки програмного забезпечення / життєвий цикл розробки системи захисту | Включають такі приклади: модель водоспаду, гнучка розробка і модель безпеки. |
|  | Мови програмування і типобезпечні мови | Обговорення проблем, які вводять мови програмування, що таке типобезпечність і чому вона має важливе значення. |
| Реалізація |  | У цьому розділі знань описуються методи включення міркувань безпеки при реалізації програмного забезпечення. |
|  | Перевірка вводу і перевірка його представлення | Ця тема включає наступне:   * Перевірка меж буферів і значення цілих чисел для того, щоб переконатися, що вони знаходяться в заданому діапазоні, * Перевірка вхідних даних, щоб переконатися, що вони є коректними і будуть коректно оброблятися. |
|  | Правильне використання API | Ця тема включає наступне:   * Переконайтеся, що параметри і середовища перевірені і контрольовані, щоб API зміг правильно застосовувати політику безпеки, * Перевірте результати використання API на наявність проблем. |
|  | Застосування засобів захисту | Ця тема включає наступне:   * Застосування криптографічної випадковості, * Правильне обмеження привілеїв процесу. |
|  | Перевірка зв’язків часу і стану | Ця тема включає наступне:   * Переконайтеся, що для файлу, який приводиться в дію, перевіряються відповідні атрибути, * Переконайтеся, що процеси запущені. |
|  | Коректна обробка виключень і помилок | Ця тема включає наступне:   * Блокувати або ставити в чергу сигнали під час обробки сигналу, якщо це необхідно, * Визначити, яку інформацію слід надати користувачеві, при цьому комбінуючи зручність використання з необхідністю приховати деяку інформацію, і як і кому повідомляти цю інформацію. |
|  | Надійне програмування | Цю тему іноді називають безпечним або захисним програмуванням. Навчальні плани повинні включати:  • Звільнення тільки виділеної пам’яті,  • Ініціалізація змінних перед використанням,  • Не покладайтеся на невизначену поведінку |
|  | Інкапсуляція структур і модулів | Ця тема містить класи та інші реалізації об’єкта. Приклад: ізоляція процесів. |
|  | Врахування середовища | Приклад: не розміщуйте конфіденційну інформацію у вихідний код. |
| Аналіз і тестування  [*Див. для отримання додаткової інформації також галузь знань «Захист компонентів», стор. 29*] |  | Цей розділ знань містить рекомендації з тестування для перевірки відповідності програмного забезпечення встановленим (і невстановленим) вимогам і специфікаціям з безпеки. Невстановлені вимоги включають вимоги до надійності в цілому. |
|  | Статичний і динамічний аналіз | У цій темі описуються різні методи для кожного з них, зокрема способи спільного застосування статичного і динамічного аналізу, а також обмеження і переваги кожного з них і способи виконання цих типів аналізу на дуже великих системах програмного забезпечення. |
|  | Модульне тестування | У цій темі описується, як тестувати компоненти програмного забезпечення, наприклад модулі. |
|  | Інтеграційне тестування | У цій темі описується тестування програмних компонентів у міру їх інтеграції |
|  | Тестування програмного забезпечення | У цій темі описується, як протестувати програмне забезпечення в цілому і помістити модульне і інтеграційне тестування в належні рамки. |
| Розгортання і підтримка |  | Цей розділ знань обговорює питання безпеки при використанні програмного забезпечення, а також при його розгортанні, підтримці і видаленні. |
|  | Налаштування конфігурації | У цій темі описується, як налаштувати систему програмного забезпечення для коректної роботи. |
|  | Виправлення і життєвий цикл вразливостей | Ця тема включає в себе управління звітами про вразливості, виправлення вразливостей, тестування виправлень і поширення виправлень. |
|  | Перевірка середовища | У цій темі описується, як забезпечити відповідність середовища припущенням, зробленим у програмному забезпеченні, а якщо таке неможливе, то як впоратися з конфліктом |
|  | DevOps – інтеграція розробки і експлуатації | У цій темі поєднуються розробка і експлуатація, а також автоматизація та моніторинг обох процесів. |
|  | Припинення/виведення з експлуатації | У цій темі описується, що відбувається при видаленні програмного забезпечення та як видалити його, не викликаючи проблем з безпекою. |
| Документація |  | У цьому розділі знань описується, як вводити і включати інформацію про міркування безпеки при налаштуванні, використанні та інших аспектах використання програмного забезпечення і його підтримки (включаючи модифікації за необхідності). |
|  | Інструкція зі встановлення | Ця тема містить документацію щодо інсталяції та налаштування програмного забезпечення. |
|  | Посібники користувача та інструкції | У цій темі описуються покрокові інструкції і пам’ятки (посібники); вони повинні акцентувати увагу на будь-яких потенційних проблемах безпеки, які можуть викликати дії користувачів. |
|  | Документація з забезпечення якості | Ця тема присвячена тому, як було забезпечено коректність, і що в даному випадку означає коректність. |
|  | Документація з забезпечення безпеки | У цій темі розглядаються потенційні проблеми безпеки, способи запобігання виникненню, можливі наслідки та способи їх усунення. |
| Етика  [*Див. для отримання додаткової інформації також галузі знань «Захист організації», стор. 51, і «Захист суспільства», стор. 62*] |  | Цей розділ знань вводить етичні міркування у всі вищеперераховані галузі, тож студенти зможуть розмірковувати про наслідки вибору, пов’язаного з питаннями безпеки, і наслідки. |
|  | Етичні питання при розробці програмного забезпечення | Ця тема охоплює повторне використання коду (ліцензування), професійну відповідальність, кодекси етики, такі як Кодекс етики і професійної діяльності в галузі програмної інженерії, підготовлений ACM/IEEE-CS. |
|  | Соціальні аспекти розробки програмного забезпечення | У цій темі розглядаються міркування про вплив розроблюваного програмного забезпечення, як при коректній роботі програмного забезпечення, так і про наслідки поганої або ненадійної практики програмування. |
|  | Правові аспекти розробки програмного забезпечення | У цій темі розглядаються аспекти відповідальності щодо програмного забезпечення, нормативні акти, а також питання, пов’язані з їх дотриманням. |
|  | Розкриття вразливостей | У цій темі описується, як розкривати, кому розкривати і коли розкривати інформацію про вразливості («відповідальне розкриття»). |
|  | Що, коли і навіщо тестувати | У цій темі описуються етичні наслідки тестування, особливо у тупикових ситуаціях. |

**4.2.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Фундаментальні принципи проектування; принципи мінімальних привілеїв, відкритого проектування і абстрактної фабрики |  |
|  | Обговоріть наслідки застосування принципу відкритого проектування або секретності проектування для безпеки. |
|  | Перерахуйте три принципи безпеки. |
|  | Поясніть, чому кожен принцип важливий для забезпечення безпеки. |
|  | Визначте необхідний принцип проектування. |
| Вимоги до безпеки та роль, яку вони відіграють у процесі проектування |  |
|  | Поясніть, чому важливі вимоги до безпеки. |
|  | Визначте загальні вектори атаки. |
|  | Поясніть важливість написання безпечних і надійних програм. |
|  | Опишіть поняття конфіденційності, а також інформації, що дозволяє встановити особистість. |
| Проблеми реалізації |  |
|  | Поясніть, чому необхідна перевірка вхідних даних і знеособлення даних. |
|  | Поясніть різницю між псевдовипадковими і випадковими числами. |
|  | Поясніть відмінність між безпечним кодуванням та виправленнями і поясніть переваги використання безпечних методів кодування. |
| Статичний, динамічний аналіз |  |
|  | Поясніть різницю між статичним і динамічним аналізом. |
|  | Обговоріть проблему, яку не може виявити статичний аналіз. |
|  | Обговоріть проблему, яку не може виявити динамічний аналіз. |
| Налаштування, виправлення |  |
|  | Обговоріть необхідність оновлення програмного забезпечення для усунення вразливостей системи безпеки. |
|  | Поясніть необхідність тестування програмного забезпечення після оновлення, але до поширення виправлення. |
|  | Поясніть важливість правильного налаштування програмного забезпечення. |
| Етична поведінка, особливо при розробці, тестуванні та розкритті вразливостей |  |
|  | Поясніть концепцію того, що навіть якщо ви можете щось зробити, це не означає, що ви повинні це зробити. |
|  | Обговоріть етичні питання розкриття вразливостей. |
|  | Обговоріть етику ретельного тестування, особливо у тупикових ситуаціях. |
|  | Визначте етичні наслідки та вплив рішень щодо проектування. |

**4.3 Галузь знань: Захист компонентів**

Галузь знань з захисту компонентів зосереджена на проектуванні, закупівлі, тестуванні, аналізі та обслуговуванні компонентів, інтегрованих в більш великі системи.

Безпека системи частково залежить від безпеки її компонентів. Безпека компонента залежить від того, як він спроектований, виготовлений, закуплений, протестований, з’єднаний з іншими компонентами, що використовується, і підтримується. Ця галузь знань в першу чергу пов’язана з аспектами безпеки проектування, виготовлення, закупівлі, тестування та аналізу компонентів. Разом з галузями знань «Захист з’єднань» і «Захист системи», галузь знань з захисту компонентів розглядає питання захисту з’єднань компонентів і їх використання в більш великих системах.

**4.3.1 Розділи знань і теми**

У наступній таблиці перераховані основні поняття, розділи знань і теми галузі знань з захисту компонентів.

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ КОМПОНЕНТІВ** | | |
| **Основні поняття**  - Уразливості компонентів системи,  - Життєвий цикл компонента,  - Принципи безпечного проектування компонентів,  - Безпека управління ланцюжками поставок,  - Тестування безпеки,  - Зворотна розробка. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Проектування компонентів  [*Див. для отримання додаткової інформації також галузь знань «Захист програмного забезпечення», стор. 23*] |  | Цей розділ знань знайомить з принципами і методами проектування, які підвищують захист компонентів. |
|  | Безпека проектування компонентів | У цій темі розглядаються загрози безпеки продуктів проектування компонентів (наприклад, схем, таблиць з’єднань та масок), такі як апаратні трояни, піратство в галузі інтелектуальної власності, зворотна розробка, несанкціонований доступ, аналіз сторонніх каналів і підробка. У ній також описуються методи захисту компонентів від несанкціонованого доступу та використання. |
|  | Принципи безпечного проектування компонентів | У цій темі розглядаються такі принципи, як створення надійної політики безпеки, розглядаючи при цьому безпеку як невід’ємну частину проектування системи, надійні обчислювальні платформи, ланцюжок сертифікатів, зниження ризику, багаторівнева безпека, простота проектування, мінімізація елементів системи, яким можна довіряти, і уникнення застосування зайвих механізмів безпеки. |
|  | Ідентифікація компонентів | У цій темі розглядаються такі методи, як водяні знаки, зняття відбитків пальців, облік, зашифровані ідентифікатори та фізично не клоновані функції для захисту компонентів від крадіжки інтелектуальної власності та забезпечення оригінальності компонентів. |
|  | Методи боротьби зі зворотною розробкою | У цій темі розглядаються такі методи, як обфускація і маскування для того, щоб проектування і реалізацію компонентів було важко повторити. |
|  | Зниження ризику атаки сторонніми каналами | У цій темі розглядаються методи захисту від атак сторонніми каналами, спрямованих в першу чергу на криптографічні алгоритми. Методи захисту включають зменшення витоку, оперативну перевірку чутливості за допомогою шумового сигналу, часті оновлення ключа, фізичні випадкові функції і безпечні ланцюги сканування. |
|  | Методи захисту від несанкціонованого доступу | У цій темі розглядаються методи створення компонентів, стійких до фізичних та електронних атак, зокрема методи фізичного захисту, системи захисту від несанкціонованого доступу і системи з сигналізацією про спроби несанкціонованого доступу. |
| Закупівля компонентів |  | Цей розділ знань описує методи забезпечення захисту компонентів системи протягом усього процесу закупівель. |
|  | Ризики ланцюга поставок | У цій темі описуються загрози безпеки і ризики для апаратного та програмного забезпечення при закупівлі компонентів. |
|  | Захист ланцюга поставок | У цій темі описуються такі стратегії, як фізичний захист, поділ виробництва, простежуваність, огляд і перевірка вантажів, а також перевірки для виявлення і запобігання порушень при забезпеченні безпеки компонентів у процесі закупівель. |
|  | Перевірка постачальників | Ця тема включає такі стратегії, як атестація постачальників для виявлення надійних постачальників і перевізників компонентів. |
| Тестування компонентів  [*Див. для отримання додаткової інформації також галузь знань «Захист програмного забезпечення», стор. 23*] |  | Цей розділ знань знайомить з методами модульного тестування і описує інструменти та методи, використовувані для тестування параметрів безпеки компонента. |
|  | Принципи модульного тестування | У цій темі описуються інструменти і методи модульного тестування, які відрізняються від тих, що застосовуються для тестування на рівні системи. |
|  | Тестування безпеки | У цій темі описуються засоби і методи, такі як тестування, що полягає в передачі на вхід неправильних, несподіваних або випадкових даних, для перевірки параметрів безпеки компонента за межами його функціональної коректності. |
| Зворотна розробка компонента |  | Цей розділ знань описує методи визначення проектування і функціональності компонента при неповній інформації. |
|  | Зворотна розробка проектування | У цій темі описуються інструменти й методи визначення проектування компонента на певному рівні абстракції. |
|  | Зворотна розробка апаратного забезпечення | У цій темі описуються інструменти й методи визначення функціональних можливостей та інших властивостей обладнання компонента, наприклад функцій інтегральної схеми. |
|  | Зворотна розробка програмного забезпечення | У цій темі описуються інструменти і методи, такі як статичний і динамічний аналіз, для визначення функціональних можливостей і властивостей програмного забезпечення компонента. |

**4.3.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Вразливості компонентів системи |  |
|  | Поясніть, як безпека компонентів системи може вплинути на безпеку системи. |
|  | Опишіть, яким чином може бути порушена конфіденційність розробки компонента. |
|  | Опишіть способи отримання інформації про функціональність компонента за наявності обмеженої інформації про його розробку та реалізацію. |
| Життєвий цикл компонента |  |
|  | Перелічіть етапи життєвого циклу компонента. |
| Принципи безпечного проектування компонентів |  |
|  | Перерахуйте продукти проектування компонентів, які можуть потребувати захисту. |
|  | Наведіть приклади декількох принципів безпечного проектування компонентів і поясніть, як кожен з них забезпечує захист компонентів. |
|  | Опишіть кілька методів захисту конструктивних елементів інтегральної схеми. |
| Управління ланцюгами поставок |  |
|  | Перелічіть загальні точки вразливості в ланцюжку поставок компонента. |
|  | Опишіть ризики безпеки в ланцюжку поставок компонентів. |
|  | Опишіть способи зниження ризиків у ланцюжку поставок. |
| Тестування безпеки |  |
|  | Поясніть різницю між модульним і системним тестування. |
|  | Перерахуйте кілька методів тестування параметрів безпеки компонента. |
| Зворотна розробка |  |
|  | Перерахуйте причини, чому хтось може перепроектувати компонент. |
|  | Поясніть різницю між статичним і динамічним аналізом при зворотній розробці програмного забезпечення. |
|  | Опишіть спосіб зворотної розробки функціональності інтегральної схеми. |

**4.4 Галузь знань: Захист з’єднань**

Галузь знань з захисту з’єднань зосереджена на захисті з’єднань між компонентами, включаючи фізичні і логічні з’єднання.

Дуже важливо, щоб кожен фахівець з кібербезпеки володів базовими знаннями в галузі цифрових комунікацій і мереж. З’єднання - це те, як взаємодіють компоненти. Більша частина цього матеріалу може бути представлена через приклади з подальшим виведенням основних понять і введенням відповідної лексики. Разом з галузями знань «Захист компонентів» і «Захист системи», галузь знань «Захист з’єднань» розглядає питання безпеки з’єднання компонентів і їх використання в більш великих системах.

**4.4.1 Розділи знань і теми**

У наступній таблиці перераховані основні поняття, розділи знань і теми галузі знань з захисту з’єднань.

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ З’ЄДНАНЬ** | | |
| **Основні поняття**  - Системи, архітектура, моделі і стандарти,  - Інтерфейси фізичних компонентів,  - Інтерфейси програмних компонентів,  - Атаки на з’єднання,  - Атаки на канали передачі. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Фізичне середовище |  | Цей розділ знань знайомить з поняттями фізичної передачі сигналів та каналами передачі. Ці загальні поняття можна пояснити за допомогою представлення історії протоколів Ethernet, бездротового 802.11. Починаючи з широкомовного домену з коаксіальним кабелем і CSMA / CD, переходячи до концентраторів, а потім комутаторів без зміни адресації і корисного навантаження. Впровадження комутації вимагає моделювання характеру мовлення для імітації характеру коаксіального мовлення. Бездротовий зв’язок – це розподілене середовище, але фізичні характеристики середовища вимагали інших механізмів запобігання конфліктів, ніж коаксіальне. |
|  | Передача у середовищі | Ця тема охоплює передачу сигналів через коаксіальний кабель, виту пару, оптичне волокно і повітря. |
|  | Розподілене середовище і середовище з’єднання «точка-точка» | У цій темі розглядаються характеристики передачі даних у цих середовищах. |
|  | Моделі спільного доступу | У цій темі описуються різні схеми спільного використання середовища декількома клієнтами. Наприклад: 802.1 Mac-адреси і PPP. |
|  | Загальні технології | У цій темі розглядаються різні реалізації описаних вище моделей. IEEE 802.3 (Ethernet), IEEE 802.11 (Wi-Fi), IEEE 802.16 (фіксований бездротовий широкосмуговий зв’язок). |
| Фізичні інтерфейси та з’єднувачі |  | Цей розділ знань описує характеристики з’єднувачів, матеріали, з яких вони виготовлені, і стандарти, що визначають характеристики з’єднувачів. Різні матеріали мають різні характеристики і здатність передавати сигнал. Навіть люди без технічної освіти повинні розуміти, що оптичне волокно відрізняється від витої пари і що кожен з них має різні стандарти і конкретні стандартні з’єднувачі. |
|  | Характеристики обладнання і матеріалів | У цій темі представлені характеристики з’єднання різних середовищ і вимоги до фізичних з’єднань. |
|  | Стандарти | У цій темі розглядаються різні стандарти для з’єднувачів. |
|  | З’єднувачі загального застосування | RJ 11, Rj 45, ST, SC, MTRJ, шина SFF IS тощо. |
| Архітектура апаратного забезпечення |  | Цей розділ знань охоплює переваги і потенційні уразливості стандартних архітектур апаратного забезпечення. |
|  | Стандартна архітектура | У цій темі описується поняття стандартної архітектури і переваги стандартизації. Історія розвитку материнських плат ПК може бути використана в якості прикладу, що показує еволюцію від ISA до PCI і далі. Можливість додавати функціональність без зміни базової архітектури карти має важливе значення. Додавання багатопортових Ethernet портів в карту дозволяє ПК стати маршрутизатором. |
|  | Стандарти апаратного інтерфейсу | У цій темі представлені різні стандарти апаратного інтерфейсу, починаючи з проектування корпусу інтегральної мікросхеми, потім шини ISA і PCI для платформ інтеграції і закінчуючи мережевими стандартами IEEE 802.3. |
|  | Загальна архітектура | У цій темі розглядаються сучасні технології, з якими зіткнуться студенти (мікросхеми процесора, материнська плата ПК, стандарти Ethernet). |
| Архітектура розподілених систем |  | Цей розділ знань знайомить із загальними поняттями розподілених систем та їх з’єднанням. Інтернет - не єдина мережа, TCP / IP - не єдиний протокол для з’єднання системи. Кожна реалізація має свої особливості і різні потенційні вразливості. Основна увага в навчальному плані має приділятися подібностям, відмінностям і причинам проектних рішень. Кожна архітектура має свої переваги та недоліки у конкретних випадках використання, а також свої вразливості й сильні сторони з погляду безпеки. Не можна припускати, що стратегія зниження ризиків для Інтернету підійде для суперкомп’ютерної інфраструктури. |
|  | Загальні поняття | У цій темі слід почати з поняття процесу в операційній системі, а потім представити різні архітектури для запуску процесів і забезпечення їх зв’язку. Симетрична багатопроцесорна обробка і загальна пам’ять, мережева модель з міжпроцесною взаємодією. |
|  | Всесвітня павутина | У цій темі розділі розглядається протокол HTTP / HTTPS і приводиться в якості прикладу стандарту розподіленої обробки. |
|  | Інтернет | У цій темі розглядається еволюція Інтернету як розподіленої платформи обробки даних. Студенти повинні чітко розуміти, чому поняття Всесвітня павутина і Інтернет не еквівалентні. |
|  | Протоколи і рівні | Ця тема охоплює 7 рівнів моделі OSI разом з 5-рівневою моделлю Інтернету і порівнює їх як приклад інкапсуляції і багаторівневості для забезпечення умов для сервісів, які будуються один на одному. |
|  | Високопродуктивні обчислення - HPC (суперкомп’ютери) | У цій темі представлені HPC і сценарії використання, що відрізняють HPC від стандартного Інтернету. |
|  | Гіпервізори і реалізації хмарних обчислень | У цій темі розглядаються концепції надання інфраструктури як послуги (IaaS), програмного забезпечення як послуги (SaaS), платформи як послуги (PaaS), а також всі їхні форми, які повинні знати студенти. |
|  | Вразливості і приклади експлойтів | У цій темі розглядаються поверхні атак різних моделей розподілених обчислень, підкреслюючи той факт, що кожен інтерфейс містить потенційні вразливості. Необхідно розглянути такі поняття, як гіпервізор, віртуальна мережа, фізична мережа і міжпроцесна взаємодія. |
| Архітектура мережі |  | Цей розділ знань вводить поняття, які, зазвичай, розглядаються в курсі комп’ютерних мереж. Він закладає основу для більш спеціалізованих розділів знань. |
|  | Загальні поняття | Ця тема охоплює поняття вузлів і периферійних пристроїв з назвами різних топологій і характеристиками передачі топологій. |
|  | Загальні архітектури | У цій темі розглядається архітектура мережі IEEE 802 і способи іменування різних мереж на підставі фізичних характеристик (LAN, MAN і т.д.) |
|  | Переадресація | У цій темі розглядається перенаправлення пакетів в цілому. Оскільки аналогічні мікросхеми тепер використовуються в маршрутизаторах і комутаторах, а SDN обробляє переадресацію окремо від побудови таблиці переадресації, це окрема тема. |
|  | Маршрутизація | У цій темі розглядаються алгоритми маршрутизації і пояснюється, як таблиці переадресації будуються з використанням алгоритмів аналізу графа, таких як стан каналу і вектор відстані. |
|  | Комутація/ з’єднання за допомогою моста | У цій темі розглядаються алгоритми навчання і стандарт з’єднання за допомогою моста IEEE 802.1, а також протокол кістякового дерева STP і його зв’язок з маршрутизацією. У даний час незрозуміло, як ця тема буде розвиватися з заміною STP в результаті появи Trill і STP. |
|  | Нові тенденції | Ця тема охоплює нові технології та їх вплив у міру появи. У даний час вплив SDN і додавання маршрутизації до рівня 2 з розширеними мостами навчання може стати змістом цієї теми. Ці технології швидко розвивається. |
| [*Див. для отримання додаткової інформації також галузь знань «Захист системи», стор. 39*] | Віртуалізація і архітектура гіпервізора | Віртуалізація надає способи проектування архітектури з використанням або власної віртуалізації (тип 1), або віртуалізації під управлінням операційної системи хоста (тип 2). |
| Реалізації мережі |  | У цьому розділі знань розглядаються конкретні технології, що реалізують загальні концепції мережевої взаємодії. Концепції мережевої архітектури можуть бути проілюстровані конкретними реалізаціями, але слід чітко вказати, що існують і інші можливості. Слід підкреслити, що вразливості використовуються в реалізаціях. Часто архітектура може бути теоретично перевірена і коректна, але реалізована таким чином, що має уразливості. Також шви між технологіями часто відкривають уразливості. Атака з використанням протоколу ARP є чудовим прикладом того, як шов між технологіями відкриває уразливості. |
|  | Мережі IEEE 802 / ISO | Ця тема присвячена детальному вивченню стандартів ISO. Очікується, що ця тема буде представлена в рамках інших курсів |
|  | Мережі IETF і TCP/IP | Ця тема присвячена детальному вивченню базової інфраструктури Інтернету і TCP. |
|  | Практична інтеграція і з’єднувальні протоколи | У цій темі розглядається проблема інтеграції технологій за допомогою реалізації того, що можна назвати інтерфейсними оболонками або з’єднувальним кодом. ARP є очевидним прикладом. Для зіставлення IP-адреси моделі міжмережевої взаємодії IETF з MAC-адресою базових мереж потрібен був певний механізм. ARP - це з’єднувальний «клей». Точно так само Infiniband потребує оболонку сумісності для передачі IP-трафіку. Інших прикладів доволі багато. |
|  | Уразливості і приклади експлойтів | У цій темі наведені приклади технологій, важливих для програми. Якщо взяти ARP за приклад, атака з використанням протоколу ARP як різновид атаки MitM є ефективною. USB та інші послідовні з’єднання можуть також надати приклади. |
| Мережеві сервіси |  | Цей розділ знань досліджує різні моделі, що використовуються для реалізації зв‘язку між споживачем сервісу і постачальником сервісу. Кожна тема може бути вивчена на багатьох рівнях з великою кількістю прикладів (наприклад, проблеми бездротового зв’язку, пов’язані з біомедичними пристроями). Цей розділ поділено, тому що сервісні моделі можуть бути реалізовані багатьма способами з великою кількістю різних архітектур. Віддалені виклики процедур (RPC) реалізуються в різних технологіях підключення, абсолютно різноманітних від процесу до процесу в одному процесорі до Інтернету. Проблеми безпеки різні, і компроміси у проектуванні змінюються на основі реалізацій і вимог. |
|  | Концепція сервісу | Ця тема представляє собою мережецентричне занурення в одну модель розподілених обчислень. Сервіс - це процес, який надає щось іншому процесу на підставі запиту. |
|  | Сервісні моделі (клієнт-сервер, однорангова мережа) | У цій темі розглядається мережецентричний підхід до моделювання сервісів. З точки зору мережі клієнт ініціює з’єднання, а сервер відповідає. З P2P будь-яка сторона може ініціювати запит. |
|  | Концепції протоколів сервісів (IPC, API, IDL) | У цій темі описані всі способи з’єднання компонентів. Виклики процедур, IPC-запити, мови визначення інтерфейсу з заглушкою, приватні протоколи через сокет, інше. |
|  | Архітектура сервісу загального зв’язку | У цій темі розглядаються конкретні служби та способи реалізації їхніх протоколів. Прикладами є SMTP, HTTP і SNMP, REST, CORBA тощо. Можна також розглянути спеціальні з’єднання, такі як бездротове управління імплантованими медичними пристроями. |
|  | Віртуалізація сервісів | У цій темі розглядається віртуалізація сервісів як метод емуляції поведінки певних компонентів, таких як хмарні додатки і сервіс-орієнтована архітектура. |
|  | Уразливості і приклади експлойтів | У цій темі розглядаються уразливості і експлойти клієнт-серверних, однорангових мережевих сервісів і сервісів віртуалізації. Сигнатури сервісів загального користування часто використовуються для профілювання вразливостей. |
| Захист мережі |  | Цей розділ знань відображає сучасні концепції мережевої безпеки. Цілком ймовірно, що з часом терміни і технології значно зміняться. Ключові поняття повинні включати в себе уразливості з’єднань, такі як несанкціоноване підключення до з’єднувача і надання можливості підслуховування. Все це призводить до уразливостей, які можуть бути використані для атаки посередника. Поняття захоплення магістральної лінії та моніторингу відхилень від бази підлягають вивченню, оскільки воно застосовується в декількох конкретних темах. |
|  | Захист мережі | У цій темі розглядаються способи захисту мережі від несанкціонованого доступу. |
|  | Реалізація IDS / IPS | У цій темі розглядаються служби виявлення і запобігання вторгнень. Ці служби проводять перевірку мережевого трафіку. |
|  | Реалізація брандмауерів і віртуальних приватних мереж (VPN) | У цій темі розглядається установка і використання брандмауерів і віртуальних приватних мереж. |
|  | Глибокоешелонований захист | У цій темі представлене поняття про те, що захист має бути багаторівневим. |
|  | Приманки і пастки | У цій темі представлене поняття впровадження навмисно вразливих мереж і пристроїв в ізольовані мережі, щоб їх можна було відстежувати і аналізувати при атаці. |
|  | Моніторинг мережі | У цій темі описуються засоби і методи моніторингу мережевих пристроїв і їхніх журналів. |
|  | Аналіз мережевого трафіку | У цій темі описуються засоби і методи отримання та аналізу пакетів, що проходять через мережу. Тема дослідження в цій галузі включає пошук загроз та виявлення шаблонів атак. |
|  | Мінімізація уразливості (поверхня атаки і вектори) | У цій темі розглядаються інструменти і методи пошуку і мінімізації вразливостей шляхом аналізу потенційних слабких місць. |
|  | Управління мережевим доступом (внутрішнє і зовнішнє) | У цій темі описуються засоби і методи обмеження потоку пакетів на основі правил для вмісту пакетів. Приклади включають технології контролю доступу до мережі; машинні сертифікати; методи профілювання машин; зондування з SNMP, DHCP, HTTP, DNS, LDAP і NMAP. |
|  | Демілітаризовані зони або DMZ / проксі-сервери | У цій темі розглядаються інструменти і методи глибокої реалізації глибокоешелоноваго захисту з використанням ізольованих мереж і спеціальних серверів. |
|  | Розробка і застосування мережевої політики | У цій темі описується процес розробки політик, які надають рекомендації та вимоги для сервісів, що надаються мережею, а також заходи, які будуть використовуватися для забезпечення дотримання політик. |
|  | Мережеві робочі процедури | У цій темі розглядається створення процедур, що використовуються для роботи в мережі. |
|  | Мережеві атаки (наприклад, перехоплення сеансу, атака посередника) | У цій темі розглядаються інструменти та методи, використовувані для тестування мережі з фактичною спробою використовувати уразливості. |
|  | Пошук загроз і машинне навчання | У цій темі описується, як пошук можливих загроз використовує машинне навчання для виявлення закономірностей у векторах атак. |

**4.4.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Системи, архітектура, моделі і стандарти |  |
|  | Обговоріть необхідність загальних моделей і архітектур для опису систем. |
|  | Опишіть модель систем, що складається з компонентів і інтерфейсів для з’єднання. |
|  | Поясніть, чому для компонента потрібен хоча б один інтерфейс. |
|  | Перерахуйте кілька стандартів, що визначають моделі, що складаються із систем компонентів і інтерфейсів. |
|  | Опишіть компоненти і інтерфейси наданого мережевого стандарту. |
| Фізичні інтерфейси компонентів |  |
|  | Поясніть, чому апаратний пристрій завжди моделюється фізичним компонентом. |
|  | Перерахуйте кілька прикладів фізичних інтерфейсів компонентів з відповідними уразливостями. |
|  | Опишіть використання вразливості наданого фізичного інтерфейсу. |
| Програмні інтерфейси компонентів |  |
|  | Поясніть, чому кожен фізичний інтерфейс має відповідний програмний компонент для забезпечення відповідного програмного інтерфейсу. |
|  | Поясніть, як компоненти програмного забезпечення організовані для представлення логічних рівнів у стандартній моделі. |
|  | Обговоріть, як 5-рівневу модель Інтернету можна розглядати як програмні компоненти та інтерфейси, що представляють рівні сервісів, інкапсульовані службами нижчого рівня. |
|  | Обговоріть, як TCP / IP, як сервіс, представлений різними інтерфейсами в різних програмних системах. |
| Атаки на з’єднання |  |
|  | Поясніть, як атаки на з’єднання можна розглядати з точки зору атак на програмні інтерфейси компонентів. |
|  | Опишіть, як зазначений стандартний інтерфейс може мати уразливості в програмному компоненті, що реалізує інтерфейс. |
|  | Опишіть, як реалізація може захистити себе від зазначеної уразливості в зазначеному стандартному інтерфейсі. |
| Атаки на канали передачі  [Див. для отримання додаткової інформації також галузь знань «Захист даних», стор 16.] |  |
|  | Поясніть, як атаки на канали передачі часто реалізуються як атаки на компоненти, які надають послугу ретрансляції інформації. |
|  | Опишіть атаки на вказаний вузол в мережі TCP/IP з описом уразливості. |
|  | Поясніть, чому атаки на канали передачі часто можна розглядати як атаки на мережеві компоненти (фізичні чи програмні). |

**4.5 Галузь знань: Захист системи**

Галузь знань з захисту системи фокусується на аспектах безпеки систем, що складаються з компонентів та з’єднань, а також використовують програмне забезпечення. Розуміння безпеки системи потребує її вивчення не тільки як набору компонентів та з’єднань, але і як цілісного модулю самого по собі. Це вимагає цілісного погляду на систему. Разом з галузями знань з захисту компонентів та з’єднань, галузь знань з захисту системи розглядає питання безпеки з’єднання компонентів і їх використання в більш великих системах.

**4.5.1 Розділи знань і теми**

У наступній таблиці перераховані основні поняття, розділи знань і теми галузі знань з захисту системи.

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ СИСТЕМИ** | | |
| **Основні поняття**  - Цілісний підхід,  - Політика безпеки,  - Автентифікація,  - Керування доступом,  - Моніторинг,  - Відновлення,  - Тестування,  - Документація. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Системне мислення |  | Цей розділ знань знайомить студентів з осмисленням системи як одного цілого, а не просто з рядом з’єднаних компонентів. |
|  | Що таке система? | У цій темі розглядається визначення поняття «система» та його залежність від контексту. |
|  | Що таке системна інженерія? | У цій темі розглядається цінність наявності хороших продуктів системної інженерії для інформування управління ризиками безпеки. |
|  | Цілісні підходи | У цій темі розглядається система в цілому, а не просто набір взаємопов’язаних компонентів. Наприклад, розгляд людських, організаційних та екологічних міркувань в цілому на відміну від розгляду кожного окремого компонента та зв’язку і того, як вони впливають на бачення ризиків. |
|  | Безпека систем загального призначення | У цій темі розглядаються питання безпеки обчислювальних систем і систем в цілому. |
|  | Безпека систем спеціального призначення | У цій темі розглядаються питання безпеки, що випливають з цілей, для яких призначена система. |
|  | Моделі загроз | У цій темі описується, які проблеми безпеки можуть виникнути, і як вони можуть бути реалізовані, виявлені і усунені. |
|  | Аналіз вимог | У цій темі представлені формування та перевірка вимог протягом усього життєвого циклу системи, зокрема в різних методологіях, таких як водоспадна і гнучка методології розробки. |
| [*Див. для отримання додаткової інформації також галузь знань «Захист програмного забезпечення», стор. 23*] | Фундаментальні принципи | Галузь знань з захисту програмного забезпечення докладно охоплює ці принципи, але вони також застосовуються і тут. |
|  | Розробка для тестування | У цій темі розглядається проектування систем для простоти і ефективності тестування. |
| Управління системою |  | У цьому розділі знань описуються методи включення міркувань безпеки при управлінні системою. |
|  | Моделі політики | У цій темі наведено такі приклади, як моделі Белла-Лападули (Bell – LaPadula), Кларка-Вілсона (Clark-Wilson), «китайської стіни» і безпеки в медичних інформаційних системах. |
|  | Курс політики | У цій темі розглядаються обмеження |
|  | Використання автоматизації | Ця тема включає інтелектуальний аналіз даних, машинне навчання і пов’язані методи, а також їх переваги та обмеження. |
| [*Див. для отримання додаткової інформації також галузь знань «Захист програмного забезпечення», стор. 23*] | Виправлення і життєвий цикл уразливостей | У цій темі розглядаються проблеми безпеки, що виникають при виправленні системи, виправленні запущеної системи, а також при обробці звітів про уразливості. |
|  | Експлуатація | У цій темі розглядається безпека при експлуатації і важливість зручності використання. |
|  | Введення в експлуатацію та виведення з експлуатації | У цій темі описуються проблеми безпеки при інсталяції і видаленні системи. |
|  | Внутрішня загроза | У цій темі наводяться приклади внутрішніх (інсайдерських) загроз, таких як просочування даних і саботаж, а також розглядаються контрзаходи. |
|  | Документація | У цій темі описується документація з безпеки і її забезпечення, а також інструкції зі встановлення та експлуатації, присвячені самій системі. |
|  | Системи і процедури | У цій темі розглядаються процедури, які використовуються для управління системами. |
| Доступ до системи  [*Див. для отримання додаткової інформації також галузь знань «Захист людини», стор. 44*] |  | У цьому розділі знань розглядаються проблеми безпеки керування доступом до систем. Він займається ідентифікацією сутностей і підтвердженням цієї ідентифікації до бажаного рівня деталізації. Теми перетинаються з галуззю знань з захисту людини, але основна увага тут приділяється елементам системи, а не людині. |
|  | Методи автентифікації | Методи автентифікації відносяться до автентифікації «людина-система» або «система-система»; приклади включають паролі, біометричні дані, ключі і єдиний вхід. |
|  | Особистість | Як особистість представляється системі? Ця тема містить ролі, імена тощо. |
| Управління системою |  | Цей розділ знань вивчає проблеми безпеки, пов’язані з управлінням самою системою. Включає в себе виявлення, компенсацію, захист і запобігання атак. |
| [*Див. для отримання додаткової інформації також галузь знань «Захист даних», стор. 16*] | Керування доступом | У цій темі основна увага приділяється керуванню доступом до ресурсів та цілісності елементів управління, а не керуванню доступом до даних, що розглядається у галузі знань з захисту даних. |
|  | Моделі авторизації | У цій темі розглядається керування авторизацією у багатьох системах, а також відмінність між автентифікацією і авторизацією. |
|  | Виявлення вторгнень | У цій темі розглядаються аномалії, неправильне використання (на основі правил, сигнатур) і методи на основі специфікацій. |
|  | Атаки | У цій темі розглядаються моделі атак (наприклад, дерева і графіки атак) і конкретні атаки. |
|  | Захист | У цій темі наведено такі приклади, як ASLR, стрибкоподібна передача IP-адрес і допуск вторгнень. |
|  | Аудит | У цій темі розглядаються ведення журналу, аналіз журналу і зв’язок з виявленням вторгнень. |
|  | Шкідливі програми | У цій темі наведено приклади комп’ютерних вірусів, черв’яків, програм-вимагачів і інших шкідливих програм. |
|  | Моделі вразливостей | У цій темі наведено приклади RISOS і PA, а також послідовний перебір CVE і CWE. |
|  | Тестування на проникнення | Ця тема охоплює методологію гіпотези дефектів та інші форми (ISSAF, OSSTMM, GISTA, PTE тощо). |
| [*Див. для отримання додаткової інформації також галузь знань «Захист даних», стор. 16*] | Криміналістична експертиза | Ця тема присвячена вимогам до криміналістичної експертизи. |
|  | Відновлення, стійкість | Ця тема містить механізми доступності. |
| Виведення системи з експлуатації |  | Цей розділ знань вивчає, як виведення з експлуатації системи до або після закінчення її життєвого циклу може вплинути на безпеку інших систем або організації, яка використовувала систему. |
|  | Виведення з експлуатації | У цій темі розглядається, як виведення з експлуатації системи до закінчення строку її служби може вплинути на безпеку інших систем або організації, яка використовувала систему. Студент повинен розуміти наслідки видалення системи, компонентів або з’єднань в межах системи для безпеки системи в цілому. |
|  | Утилізація | Ця тема включає очищення носіїв та інші форми знищення для запобігання відновлення конфіденційної інформації (наприклад, персональних даних). |
| Тестування системи [*Див. для отримання додаткової інформації також галузі знань «Захист програмного забезпечення», стор. 23, і «Захист з’єднань», стор. 29*] |  | Цей розділ знань охоплює питання тестування систем для забезпечення їх відповідності вимогам безпеки. |
|  | Перевірка вимог | У цій темі описуються методології, які дозволяють перевірити, що вимоги відповідають цілям. |
|  | Перевірка складу компонентів | У цій темі описується тестування системи в цілому. |
|  | Модульне проти системного тестування | У цій темі розглядається відмінність системного тестування від тестування компонентів і з’єднань. |
|  | Формальна верифікація системи | Ця тема охоплює мови, системи доведення теорем та ієрархічну декомпозицію. |
| Загальні архітектури систем |  | Цей блок знань застосовує теми цієї галузі знань до конкретних архітектур, які є або стають все більш поширеними. |
| [*Див. для отримання додаткової інформації також галузь знань «Захист з’єднань», стор. 32*] | Віртуальні машини | У цій темі розглядаються гіпервізори, віртуалізація дисків і пам’яті, а також використання віртуальних машин при забезпеченні безпеки. |
|  | Промислові системи управління | Ця тема включає SCADA. |
|  | Інтернет речей (IoT) | У цій темі наведено приклади холодильників і датчиків. |
|  | Вбудовані системи | У цій темі наведено приклади систем в космічних апаратах та систем, що використовуються в інших агресивних середовищах. |
|  | Мобільні системи | У цій темі наведено приклади ноутбуків і смартфонів. |
|  | Автономні системи | У цій темі наведено приклади роботів і БПЛА, які не потребують управління людиною. |
|  | Системи загального призначення | У цій темі наведено приклади настільних комп’ютерів, ноутбуків і мейнфреймів. |

**4.5.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Цілісні підходи |  |
|  | Поясніть поняття довіри і надійності. |
|  | Поясніть, що мається на увазі під конфіденційністю, цілісністю і доступністю. |
|  | Поясніть, що таке політика безпеки та її роль у захисті даних і ресурсів. |
| Політика безпеки  [Див. для отримання додаткової інформації також галузь знань «Захист організації», стор 51.] |  |
|  | Обговоріть важливість політики безпеки. |
|  | Поясніть, чому різні сайти мають різні політики безпеки. |
|  | Поясніть взаємозв’язок між групою безпеки, конфігурацією системи та процедурами забезпечення безпеки системи. |
| Автентифікація |  |
|  | Поясніть три параметри, які зазвичай використовуються для автентифікації. |
|  | Поясніть важливість багатофакторної автентифікації. |
|  | Поясніть переваги пароля-фрази перед звичайним паролем. |
| Керування доступом |  |
|  | Опишіть список керування доступом |
|  | Опишіть фізичне і логічне керування доступом і порівняйте їх. |
|  | Поясніть відмінність між авторизацією та автентифікацією. |
| Моніторинг |  |
|  | Обговоріть, як системи виявлення вторгнень сприяють забезпеченню безпеки. |
|  | Опишіть обмеження антивірусного програмного забезпечення, наприклад антивірусних програм |
|  | Обговоріть використання моніторингу системи. |
| Відновлення |  |
|  | Поясніть, що таке стійкість і визначте середовище, в якому вона важлива |
|  | Обговоріть основи плану аварійного відновлення |
|  | Поясніть, чому резервні копії представляють потенційну загрозу безпеці. |
| Тестування |  |
|  | Опишіть, що таке тест на проникнення і чому він має важливе значення. |
|  | Обговоріть документування тесту, що виявляє вразливість. |
|  | Обговоріть важливість перевірки вимог. |
| Документація |  |
|  | Обговоріть важливість документування коректної установки і конфігурації системи. |
|  | Будьте в змозі написати документацію щодо вторгнень у мережу і головний комп’ютер-хост. |
|  | Будьте в змозі пояснити наслідки для безпеки, до яких може призвести неясна або неповна документація з експлуатації системи. |

**4.6 Галузь знань: Захист людини**

Галузь знань з захисту людини фокусується на захисті даних об особах і конфіденційності у контексті організацій (наприклад, на захисті співробітників) і особистого життя на додаток до вивчення поведінки людини стосовно кібербезпеки.

**4.6.1 Розділи знань і теми**

Люди несуть відповідальність за забезпечення конфіденційності, цілісності та доступності (CIA) своїх організаційних і персональних комп’ютерних систем, в той час як ця відповідальність залежить від кожного з розділів знань в галузі знань з захисту людини, викладених нижче. У наступній таблиці перераховані основні поняття, розділи знань і теми галузі знань з захисту людини.

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ ЛЮДИНИ** | | |
| **Основні поняття**  - Управління ідентифікацією,  - Соціальна інженерія,  - Усвідомлення і розуміння,  - Конфіденційність і безпека соціальної поведінки,  - Безпека та конфіденційність персональних даних. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Управління ідентифікацією |  |  |
|  | Ідентифікація і автентифікація людей і пристроїв | У цій темі представлено огляд різних методів керування доступом з метою продемонструвати переваги і проблеми кожного з них. Тема включає огляд керування доступом до мережі (NAC), керування доступом до ідентифікаційної інформації (IAM), ролей, систем комплексної ідентифікації і автентифікації, систем біометричної автентифікації (включаючи такі проблеми, як точність/FAR/FRR, стійкість, конфіденційність тощо), а також зручність і допустимість методів. |
|  | Керування фізичними і логічними ресурсами | У цій темі розглядаються різні засоби керування доступом до фізичних ресурсів, включаючи системне обладнання, мережні ресурси, пристрої резервного копіювання і зберігання даних тощо. Приклади: керування доступом до мережі (NAC), керування доступом до ідентифікаційної інформації (IAM), керування доступом на основі правил (RAC), керування доступом на основі ролей (RBAC), методи відстеження матеріально-виробничих запасів та методи створення ідентичності (який тип ID користувача допомагає підвищити рівень безпеки при керуванні доступом, наприклад, abc1234, ім’я та прізвище, ініціал та прізвище). |
|  | Ідентичність як послуга (IaaS) | У цій темі розглядається керування ідентифікаційною інформацією як послугою (наприклад, хмарна ідентифікація). Також розглядаються такі проблеми, як вихід системи з-під контролю користувача без можливості дізнатися, що сталося з інформацією в системі, аудит доступу, забезпечення відповідності і гнучкості для швидкого відкликання дозволів. |
|  | Сторонні служби ідентифікації | У цій темі представлено огляд інфраструктури автентифікації, що використовується для створення, розміщення та управління сторонніми службами ідентифікації. Тема включає локальні, хмарні, централізовані служби ідентифікації / засоби управління паролями, управління привілеями кінцевих точок і т.д. |
|  | Атаки на керування доступом і заходи з пом’якшення наслідків | У цій темі представлено огляд різних типів атак на керування доступом для крадіжки даних або облікових даних користувача, а також заходи щодо боротьби з ними. Тема включає такі поняття, як злом паролю, перебір за словником, метод «грубої сили» і спуфінг-атака; багатофакторна автентифікація; політика надійних паролів; файли захищених паролів; обмеження доступу до систем тощо. |
| Соціальна інженерія |  |  |
|  | Типи атак за допомогою соціальної інженерії | У цій темі представлено огляд різних способів використання кіберзлочинцями або шкідливими групами слабких місць в організаціях, системах, мережах та особистої інформації, що використовуються для забезпечення подальшої кібератаки. Пропонована тема включає: фішинг і фішингові атаки, фізична / маскування під законного користувача, вішинг (телефонний фішинг), підробка електронної пошти та цькування. |
|  | Психологія атак за допомогою соціальної інженерії | У цій темі представлено огляд психологічних і поведінкових факторів, пов’язаних з особами, що потрапляють під атаки за допомогою соціальної інженерії. Пропонована тема включає змагальний характер мислення, вплив емоційних реакцій на прийняття рішень, когнітивні упередження щодо ризиків і вигод і зміцнення довіри. |
|  | Введення користувачів в оману | У цій темі представлено огляд інтерфейсів систем обміну повідомленнями і браузерів і / або взаємодії з користувачами, які можуть використовуватися для введення користувачів в оману. Пропонована тема включає відправників спуфінг-повідомлень, URL-адреси, що вводять в оману, як користувачі оцінюють і довіряють веб-сторінкам і електронним листам, а також поведінка користувачів при отриманні фішингових і інших попереджень браузера. |
|  | Виявлення і пом’якшення наслідків атак за допомогою соціальної інженерії | У цій темі представлено практичні дії на основі сценаріїв з застосуванням моделювання або віртуальних інструментів для створення середовища різних атак за допомогою соціальної інженерії. Практичний досвід використання інструментів і технічних підходів для виявлення та / або зниження різних загроз соціальної інженерії. Пропоновані інструменти, такі як фільтрація електронної пошти, чорний список, інструменти управління інформаційною безпекою та подіями безпеки (SIEM) і IDS/IPS. |
| Особисте дотримання правил /політики / етичних норм кібербезпеки  [*Див. для отримання додаткової інформації також галузь знань «Захист суспільства», стор. 62*] |  |  |
|  | Некоректне використання системи і некоректна поведінка користувача | У цій темі представлено огляд навмисного і ненавмисного некоректнного використання системи, віртуальне залякування, кібер-злом, легковірна поведінка і етичні дилеми, пов’язані з рішеннями системи безпеки. |
|  | Примушення до виконання і правила поведінки | У цій темі представлено огляд методів та способів примушення людей дотримуватися правил / політики / етичних норм (наприклад, водіння!). Тема включає в себе наслідки за недотримання правил /політики/етичних норм у сфері кібербезпеки, документацію та журнали аудиту (докази відповідності, щоб довести, що правила / політика / етичні норми були дотримані), і знання відповідальності за недотримання правил / політики / етичних норм у сфері кібербезпеки. Стимули для збереження роботи (особливо після одержання освіти і підготовки за належними правилами/політики/етичним нормам, люди несуть юридичну відповідальність за недотримання правил в якості працівника), і люди можуть втратити свою ідентичність/доступ в особистому житті через недостатнє дотримання правил. |
|  | Правильна поведінка в умовах невизначеності | У цій темі представлено огляд методів та прийомів, яких слід дотримуватися, коли неясно, як реагувати на ситуацію, пов’язану з кібербезпекою. Тема включає CyberIQ, інтелектуальну адаптивність, критичне мислення, розуміння правильного і неправильного вибору, як зробити цей вибір в умовах невизначеності, раціональне і ірраціональне мислення, етичне мислення/рішення і поведінка, коли немає чіткого процесу, якого слід дотримуватися (звітність/контактний центр/тощо), та пом’якшення наслідків людських помилок. |
| Усвідомлення і розуміння  [*Див. для отримання додаткової інформації також галузь знань «Захист організації», стор. 51*] |  |  |
|  | Сприйняття та інформування про ризики | У цій темі описується, як користувачі сприймають ризики кібербезпеки і реагують на них, когнітивні упередження при оцінці ризиків, метафори для передачі конкретних ризиків безпеки і способи створення повідомлень про ризики. Визначення ментальної моделі, як ментальні моделі впливають на поведінку користувачів, а також загальні ментальні моделі (народні моделі) кібербезпеки і конфіденційності. |
|  | Кібергігієна | Ця тема містить дискусії та заходи, спрямовані на обов’язки людини (а не організації) щодо захисту і пом’якшення наслідків кіберзагроз та кібератак. Тема включає створення паролів, зберігання паролів, інструменти пом’якшення наслідків (наприклад, антивіруси), як визначити безпечні сайти, виявлення рівня налаштувань конфіденційності тощо. |
|  | Методи навчання користувачів | Методи навчання кінцевих користувачів різним загрозам в сфері кібербезпеки/ конфіденційності і поведінці в таких ситуаціях. Тема включає методи для підвищення обізнаності користувачів (підлітків, співробітників, громадськості тощо), методи навчання і підготовки в сфері кібербезпеки (наприклад, плакати, листівки, комп’ютерне навчання, гейміфікація, стилі спілкування, формування повідомлень, способи охоплення різних аудиторій і співтовариств користувачів, осіб з обмеженими можливостями та/або когнітивними порушеннями), строки та посилення освіти, а також вплив навчання на знання і поведінку користувачів. |
|  | Обізнаність про кібер-уразливість і загрози | У цій темі представлено огляд загроз, з якими стикаються користувачі, а також страх, невизначеність і сумнів (FUD). Запропонована тема включає ознаки уразливості внутрішнього співробітника і загроз, усвідомлення крадіжки особистих даних, підробка корпоративної електронної пошти, небезпека безкоштовних/відкритих Wi-Fi мереж і шкідливих програм, шпигунських програм і програм-вимагачів. |
| Соціальна і поведінкова конфіденційність  [*Див. для отримання додаткової інформації також галузь знань «Захист суспільства», стор. 62*] |  |  |
|  | Соціальні теорії конфіденційності | У цій темі представлено огляд різних теорій соціальної психології та соціальних наук щодо конфіденційності, зосереджуючись на конфіденційності, яка включає в себе взаємодію з іншими людьми, а не організаціями. Пропонована тема включає компроміси і ризики конфіденційності в соціальному контексті, управління і обізнаність про згоду на обробку даних, моніторинг особистої інформації, нормативні заходи захисту і проблеми соціальної підтримки конфіденційності. |
|  | Конфіденційність і безпека в соціальних мережах | У цій темі представлено огляд поведінки та проблем користувачів в області захисту особистої інформації при використанні соціальних мереж. Запропонована тема включає рішення і поведінку користувачів при розкритті інформації онлайн, керування ідентифікаційною інформацією і створеними образами, визначення керування аудиторією і доступом до соціальних мереж, інтерфейс і механізми управління конфіденційністю на різних сайтах соціальних мереж, проблеми управління обмеженнями користуванням соціальними мережами у часі, особистому житті і на робочому місці. |
| Конфіденційність і захист персональних даних  [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, і «Захист організації», стор. 51*] |  |  |
|  | Конфіденційні персональні дані (SPD) | У цій темі представлено огляд типів персональних даних (PD), зокрема інформацію, що дозволяє встановити особистість (PII), яка є особливо вразливою через ризик того, що така інформація може бути використана не за призначенням, щоб завдати значної шкоди людині у фінансовому, професійному або соціальному плані. Пропонована тема включає приклади елементів даних конфіденційних персональних даних (SPD) (номер соціального забезпечення, номер соціального страхування або інший ідентифікаційний номер, виданий урядом, такий як номер водійського посвідчення або паспорту; номер банківського рахунку; номери кредитних карт; інформація про стан здоров’я; біометричні або генетичні дані тощо), правила, що регулюють збір, використання та поширення SPD, і можливості для виведення SPD. |
|  | Відстеження особистості і цифровий слід | Відстеження місця розташування, відстеження веб-трафіку, відстеження в мережі, відстеження особистих пристроїв, записів віртуальних помічників (Сірі, Алекса і т.д.). Тема включає поведінку користувачів і проблеми, пов’язані з кожним з цих видів відстеження, а також поточні методи обмеження відстеження та захисту конфіденційності. |
| Доступний захист і конфіденційність  [*Див. для отримання додаткової інформації галузі знань «Захист організації», стор. 51, і «Захист суспільства», стор. 62*] |  |  |
|  | Зручність користування (юзабіліті) і досвід користувача | Визначення поняття юзабіліті і досвіду користувача, а також вплив, який юзабіліті (або її відсутність) мають на безпеку і конфіденційність системи. Тема включає приклади проблем зручності використання в традиційних системах забезпечення безпеки, таких як автентифікація або шифрування, зручність використання і компроміси безпеки в системах, методи оцінки зручності використання систем забезпечення безпеки та конфіденційності. |
|  | Фактори безпеки людини | Студенти зможуть працювати на перетині людської психології, інформатики та області забезпечення якості. Тож вони повинні мати глибокі знання з обчислювань і людської поведінки та забезпечення якості. Тема включає в себе прикладну психологію в контексті змагального мислення і політики безпеки, економіку безпеки, нормативно-правову базу, відповідальність, матеріальну відповідальність, самовизначення, видавання себе за іншого і шахрайство (наприклад, фішинг і цільовий фішинг, довіра, обман, опір біометричній автентифікації і управління ідентифікаційною інформацією). |
|  | Обізнаність про політику та її розуміння | У цій темі представлено огляд політик (наприклад, HIPAA, FERPA, PII) і методів, які слід використовувати при виникненні ситуації, пов’язаної з безпекою. Тема включає в себе перепідготовку при оновленні політик, перегляд існуючих загроз і перевірку знань, щоб забезпечити розуміння політики, коли справа доходить до захисту даних. У зв’язку з частковим збігом тем також слід посилатися на розділи знань в галузях знань з захисту суспільства і захисту організації. |
|  | Політика конфіденційності | У цій темі представлено огляд політик конфіденційності щодо соціальних і локальних розходженнях. Слід вивчити юрисдикційні відмінності у визначеннях політики конфіденційності. Відносини між окремими особами, організаціями чи державними політиками конфіденційності також повинні розглядатися з точки зору користувачів. Додаткові теми повинні включати вплив політики конфіденційності на нові інструменти / програмне забезпечення, виявлення необхідності використання інструментів і методів, які слід охопити в більшості галузей. Крім того, повідомлення користувачів про те, як їх дані використовуються, щоб вони могли зробити свідомий вибір щодо надання інформації. |
|  | Рекомендації щодо проектування і реалізації | Рекомендації включають зниження навантаження на користувачів і рішення, що забезпечують налаштування параметрів безпеки за замовчуванням, скорочення ненавмисних помилок безпеки та конфіденційності, контекстуальні і конкретні загрози поряд з ризиками, а також скорочення технічних термінів та жаргону. |

**4.6.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Управління ідентифікаційною інформацією |  |
|  | Поясніть різницю між ідентифікацією, автентифікацією і авторизацією доступу людей і пристроїв. |
|  | Обговоріть важливість журналу аудиту і ведення журналу при ідентифікації і автентифікації. |
|  | Продемонструйте здатність реалізувати концепцію найменших привілеїв і розподілу обов’язків. |
|  | Продемонструйте розуміння атак на керування доступом та заходів щодо пом’якшення наслідків. |
| Соціальна інженерія |  |
|  | Продемонструйте розуміння типів атак за допомогою соціальної інженерії, психології атак за допомогою соціальної інженерії і введення в оману користувачів. |
|  | Продемонструйте здатність виявляти типи атак за допомогою соціальної інженерії. |
|  | Продемонструйте можливість реалізації підходів до виявлення і пом’якшення наслідків атак за допомогою соціальної інженерії. |
| Усвідомлення і розуміння |  |
|  | Обговоріть важливість кібергігієни, навчання користувачів кібербезпеці, а також обізнаності про уразливість і загрози. |
|  | Опишіть основні теми в рамках програм навчання, підготовки та підвищення обізнаності з питань безпеки (SETA). |
|  | Обговоріть важливість SETA як контрзаходу. |
|  | Обговоріть важливість сприйняття ризику та інформування про нього в контексті ментальних моделей кібербезпеки і конфіденційності. |
| Соціальна поведінкова конфіденційність і безпека |  |
|  | Порівняйте різні теорії соціальної психології та соціальних наук щодо конфіденційності. |
|  | Опишіть концепції компромісів і ризиків конфіденційності в соціальному контексті, керування і обізнаність про згоду на обробку даних, моніторинг особистої інформації, нормативні заходи захисту і проблеми соціальної підтримки конфіденційності. |
|  | Обговоріть важливість конфіденційності та безпеки соціальних мереж. |
| Конфіденційність і безпека персональних даних |  |
|  | Обговоріть важливість захисту конфіденційних персональних даних (SPD) і інформації, що дозволяє встановити особистість (PII). |
|  | Обговоріть важливість нормативних положень, що регулюють збір, використання та поширення SPD, а також можливості для виведення SPD. |
|  | Опишіть поняття відстеження особистості та цифрового сліду, розуміючи при цьому інвазивність таких інструментів у контексті конфіденційності. |

**4.7 Галузь знань: Захист організації**

Галузь знань з захисту організації зосереджена на захисті організацій від загроз кібербезпеки і управлінні ризиками для успішного виконання місії організації. Організації несуть відповідальність за задоволення потреб багатьох груп, і ці потреби повинні бути охоплені кожною із цих груп знань.

**4.7.1 Розділи знань і теми**

Студенти повинні вміти визначати типи законів, положень і стандартів з безпеки, в межах яких працює організація. Урядова організація має набір профілів безпеки, в той час як корпоративна організація фокусується на іншому. Політика безпеки повинна відповідати поточним потребам організації і розвиватися разом з нею. Фахівець з безпеки повинен розуміти поточні правила і положення і те, як вони відповідають їх відповідним бізнес-вертикалях, таким як охорона здоров’я та електронна комерція.

У наступній таблиці перераховані основні поняття, розділи знань і теми галузі знань з захисту організації. У зв’язку з частковим збігом тем слід звертатися до розділів знань галузі знань з захисту суспільства.

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ ОРГАНІЗАЦІЇ** | | |
| **Основні поняття**  - Управління ризиками,  - Управління і політика,  - Закони, етика та їх дотримання,  - Стратегія і планування. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Управління ризиками |  | Управління ризиками - це пошук і управління ризиками для інформаційних ресурсів організації. |
|  | Виявлення ризику | Ідентифікація ресурсів - це каталогізація інформаційних ресурсів організації, таких як бази даних або апаратне забезпечення для того, щоб допомогти у виявленні ризику на випадок зламу або втрати ресурсів. Загрози включають будь-яку подію, яка використовує вразливість і яка може призвести до втрат або збитків організації. Аналіз загроз (моделювання загроз) все частіше використовується організаціями для підтримки обізнаності та потенціалу реагування на існуючі та виникаючі загрози. |
|  | Оцінка і аналіз ризиків | Аналіз ризиків - це організаційний процес визначення і усунення можливих випадкових або навмисних втрат, а також розробка та впровадження процедур для мінімізації впливу цих втрат. Також може включати аналіз загроз і дослідження загроз. |
|  | Внутрішні (інсайдерські) загрози | У цій темі розглядаються шкідливі поведінкові фактори, які можуть заподіяти шкоду внаслідок свідомого порушення довіри, практики оптимального використання або ненавмисної помилки.  *Інсайдер* визначається як будь-яка особа, що має авторизований доступ до ресурсів організації, включаючи персонал, об’єкти, інформацію, обладнання, мережі та системи.  *Інсайдерська загроза* визначається як ризик того, що інсайдер буде використовувати свій авторизований доступ, свідомо чи мимоволі, щоб завдати шкоди своїй організації. Це може включати в себе крадіжку службової інформації і технологій; пошкодження об’єктів, систем або обладнання організації; фактичну або потенційну шкоду співробітникам; або інші дії, які можуть перешкодити організації здійснювати свою звичайну ділову діяльність.  Ця тема охоплює мотив-засоби-можливості: фактори мотивації і дисципліни, відповідальність, обізнаність та контроль якості.  ФБР розробило матеріали, зокрема показники, корисні для виявлення потенційних ризиків інсайдерської загрози. |
|  | Оцінка ризику, моделі і методології оцінки ризику | Для пояснення того, як ресурси стикаються з ризиком, використовуються моделі ризиків. Крім того, існує ряд прийнятих в галузі методологій для вимірювання, оцінки та інформування зацікавлених сторін про ризики.  Ця тема включає як кількісні, так і якісні підходи до оцінки ризиків, застосування моделей і методів для різних бізнес-контекстів (наприклад, HIPAA для медичних установ). Інструменти, що представляють інтерес, можуть включати самооцінку стійкості до кіберзагроз, інструмент оцінки кібербезпеки (CSET), а також інструмент оцінки ризиків безпеки від HSS. |
|  | Управління ризиками | *Управління ризиками* визначається як заходи, спрямовані на зменшення наслідків кібер-події і, як наслідок, зменшення значення ризику. Кожен підхід повинен включати засоби інформування осіб, які приймають рішення, про ризик, включаючи *залишковий ризик*. Тема повинна включати оцінку і ранжування ризиків, а також категорії «уникнути, знизити, передати, прийняти».  Зміст навчальних планів має включати широко використовувані методології управління ризиками, доступні для вивчення і практики. |
| Управління безпекою і політика  [*Див. для отримання додаткової інформації також галузь знань «Захист суспільства», стор. 62*] |  | Кожна організація вирішує свої оперативні завдання, внутрішні і зовнішні, на основі політики і управління. Управління є обов’язком вищого керівництва організації, який має на меті забезпечення ефективного здійснення стратегічного планування, управління ризиками та дотримання нормативних вимог, як правило, з допомогою комплексної управлінської політики, планів, програм та бюджетного контролю, з тим щоб забезпечити безпеку інформації організації.  Здійснення управління і політики в галузі безпеки має здійснюватися в рамках загальних, національних і місцевих законів, положень і стандартів.  Цей розділ знань зосереджений на розумінні циклу розробки політики в галузі безпеки, починаючи з початкових досліджень і закінчуючи впровадженням та обслуговуванням, а також на ознайомленні з реальними прикладами політики і практики в галузі безпеки. |
|  | Організаційний контекст | Багато факторів впливають на функціонування безпеки в організаціях. Ці контексти мають вирішальне значення при розробці навчального плану і повинні пояснювати весь процес.  У цій темі розглядаються, як внутрішні і зовнішні контекстуальні відмінності істотно впливають на охоплення політики, регулювання і статут (або юрисдикцію). Крім того, слід провести оцінку питань і проблем, пов’язаних з місцем розташування організації або конкретною країною. Слід також провести оцінку застосовних стандартів і керівних принципів, що стосуються дотримання вимог в промисловості / секторі. Різниця між урядовими і приватними організаціями є одним з факторів, так само як і необхідність включення міжнародних аспектів, включаючи, крім іншого, обмеження на імпорт/експорт. Крім того, існує значна різниця між організаціями у різних бізнес-вертикальних сегментах промисловості, таких як енергетика і сільське господарство. |
| [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, «Захист людини», стор. 44 і «Захист суспільства», стор. 62*] | Конфіденційність | Конфіденційність є концепцією з культурними та національними варіаціями в її визначенні. За своєю суттю, конфіденційність заснована на праві бути забутим, а також на різних рівнях вибору і згоди на збір, використання і поширення інформації про людину.  У цій темі розглядаються соціальні та локалізовані відмінності щодо поняття конфіденційності. Слід вивчити юрисдикційні відмінності у визначенні конфіденційності. Відносини між окремими особами, організаціями чи державними вимогами щодо конфіденційності також повинні бути розглянуті.  Вплив налаштувань конфіденційності в нових інструментах / програмному забезпеченні, виявлення потреби в інструментах і методах, які будуть охоплені в більшості галузей.  Додаткову увагу слід приділяти питанням конфіденційності в контексті положень про захист прав споживачів та охорони здоров’я.  Організації з міжнародною участю повинні враховувати відмінності в законах, положеннях і стандартах про конфіденційність в юрисдикціях, в яких вони працюють. |
| [*Див. для отримання додаткової інформації також галузь знань «Захист суспільства», стор. 62*] | Закони, етика і їх дотримання | Закони, положення, стандарти, а також етичні цінності випливають із соціального контексту і того, як організації виконують вимоги щодо їх дотримання.  Ця тема включає в себе пояснення того, як закони і технології перетинаються в контексті судових структур - міжнародних, національних і місцевих, - які представлені як організації, що захищають свої інформаційні системи від кібератак.  Етичне виховання також має бути елементом навчання. Слід розглянути професійні кодекси поведінки та етичні стандарти. Зусилля із забезпечення дотримання повинні включати зусилля щодо приведення у відповідність до законів, положень і стандартів, а також вимоги щодо повідомлення про порушення з боку державних, національних і міжнародних керівних органів. Приклади міжнародних законів і стандартів включають GDPR і ISO / IEC 27000 та ін. Національні закони, що мають важливе значення для американських організацій, включають HIPAA, Sarbanes-Oxley, GLBA і т. д. |
|  | Управління безпекою | Принципи корпоративного управління застосовуються також і до функції інформаційної безпеки. Управління є обов’язком вищого керівництва організації, який має на меті забезпечення ефективного здійснення стратегічного планування, управління ризиками та дотримання нормативних вимог, як правило, з допомогою комплексної управлінської політики, планів, програм та бюджетного контролю, з тим щоб забезпечити безпеку інформації організації.  Ця тема повинна визначати реалізацію управління і політики в галузі безпеки в рамках загальних, національних і місцевих законів, положень і стандартів, а програми навчання повинні намагатися передати концепції з чіткими роз’ясненнями і обґрунтованими прикладами. |
|  | Інформування на рівні вищого керівництва та ради директорів | Надання інформації керівникам і третім особам, які приймають рішення, є критично важливою навичкою для керівників відділу інформаційної безпеки.  Ця тема включає в себе навички спілкування, які викладаються і практикуються з репетиціями і які включають критичний аналіз і значимий зворотний зв’язок. |
|  | Управлінська політика | Організаційні керівні принципи, які диктують певну поведінку в організації.  Ця тема повинна передати поняття з чіткими роз’ясненнями і обґрунтованими прикладами, включаючи політику програми забезпечення безпеки, політику щодо конкретних проблем і системну політику згідно NIST SP 800-12 Rev 1. Також включає розуміння циклу розробки політики забезпечення безпеки, від первинних досліджень до впровадження та супроводу, а також ознайомлення з реальними прикладами політики і практики забезпечення безпеки. |
| Аналітичні інструменти |  | Цей розділ знань являє собою набір методів, що використовують аналіз даних для розпізнавання, блокування, перенаправлення та реагування на кібератаки. Моніторинг мережевої активності в режимі реального часу дозволяє гнучко приймати рішення, виявляти підозрілі шкідливі дії, використовувати панель управління візуалізацією в реальному часі і використовувати набір апаратного і програмного забезпечення для управління такими виявленими підозрілими діями. |
|  | Вимірювання продуктивності (метрики) | Процес проектування, реалізації і управління використанням певних вимірювань для визначення ефективності загальної програми безпеки. Побудований на метриках, термін, який використовується для опису будь-якого методу детального статистичного аналізу продуктивності, але тепер зазвичай є синонімом вимірювання продуктивності.  Зміст навчальних планів має включати підходи і методи для визначення та оцінки корисності вимірювань продуктивності повинні бути пояснені студентам. |
|  | Аналіз даних | Аналіз даних - це набір методів, використовуваних для оперування (часто) великими обсягами даних для розпізнавання, блокування, перенаправлення та реагування на кібератаки. Моніторинг мережевої активності в реальному часі дозволяє швидко приймати рішення, виявляти підозрілі шкідливі дії, використовувати панель управління візуалізацією в реальному часі і використовувати набір апаратного і програмного забезпечення для управління виявленими підозрілими діями.  Ця тема містить визначення; відмінності між програмним забезпеченням і інструментами для управління безпекою та аналізу забезпечення безпеки; тип і класифікація аналітичних інструментів і методів (з прикладами, такі як OpenSOC); збір, фільтрацію, об’єднання і зв’язок інформації про різні типи подій безпеки; як працюють інструменти аналізу забезпечення безпеки; взаємозв’язок між аналітичним програмним забезпеченням та інструментами і криміналістичною експертизою; відмінності між інструментами криміналістичної експертизи та аналітичними інструментами; мережева криміналістика (включаючи аналіз пакетів, інструменти, Windows, Linux, Unix, мобільне програмне забезпечення); відмінності між кібер-криміналістикою (наприклад, соціальні мережі) і мережевою криміналістикою. |
|  | Аналіз безпеки | Збір, аналіз і поширення інформації про безпеку, включаючи, але не обмежуючись, погрозами і можливостями противника.  У цій темі слід вивчити інструменти і методи збору та агрегування даних, інтелектуального аналізу даних, аналізу даних, статистичного аналізу. Приклади джерел аналізу безпеки включають SIEM для внутрішніх даних та державні і приватні аналітичні служби для зовнішніх даних. Поширення включає в себе розуміння підходу Центру обміну інформацією та аналізу, а також таких організацій, як InfraGard. |
| Адміністрування системи |  | Адміністрування системи працює за лаштунками для налаштування, експлуатації, обслуговування та усунення недоліків технічної інфраструктури системи, яка підтримує більшу частину сучасного життя.  Необхідні знання: базові знання про комп’ютерні системи (Windows / Linux), мережі (модель OSI), програмне забезпечення і бази даних (Oracle/SQL). |
|  | Адміністрування операційної системи | У цій темі розглядаються питання технічного обслуговування, надійної роботи, налаштування та усунення несправностей технічних систем, особливо систем і серверів з багатьма користувачами.  Ця тема включає, крім іншого, управління обліковими записами, адміністрування дисків, системних процесів, автоматизація завдань системи, моніторинг продуктивності, оптимізація, адміністрування інструментів з забезпечення безпеки і резервного копіювання дисків і процесу. |
|  | Адміністрування баз даних | У цій темі розглядається управління базами даних і їх обслуговування за допомогою доступного і застосовного програмного забезпечення системи управління.  Ця тема включає, крім іншого, встановлення та налаштування серверів баз даних, створення схем, таблиць, індексів, представлень, обмежень, збережених процедур, функцій, створення облікових записів користувачів і адміністрування, а також засоби резервного копіювання і відновлення баз даних. Тема повинна включати широко використовувані технології зберігання даних, а також нові технології управління даними. |
|  | Адміністрування мережі | Адміністрування мережі відноситься до встановлення і підтримки різних мережевих архітектур систем (LAN, WAN Man, інтранет, екстранет, демілітаризовані зони тощо) і інших систем передачі даних.  Ця тема включає, крім іншого, модель OSI, захист мережевого трафіку і засоби налаштування сервісів. |
| [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, «Захист людини», стор. 44 і «Захист суспільства», стор. 62*] | Адміністрування хмарної інфраструктури | Адміністрування хмарної інфраструктури - це обслуговування та забезпечення надійного доступу до динамічного пулу віддалених ресурсів (наприклад, мережі, сервери, сховища, додатки і сервіси), які можна швидко налаштувати, підготувати і випустити з мінімальним контролем.  Ця тема включає, крім іншого, налаштування й розгортання додатків у хмарних інфраструктурах, аналіз продуктивності, масштабування ресурсів, доступність хмарних платформ, виявлення проблем безпеки та конфіденційності та зниження ризиків. |
|  | Адміністрування кіберфізичних систем | Кіберфізичні системи (CPS) - це інженерні системи, побудовані на основі безшовної інтеграції обчислювальних алгоритмів і фізичних компонентів і залежні від них. Адміністрування CPS відноситься до установки і обслуговування шляхом забезпечення безпеки, функціональності, адаптивності, масштабованості, відмовостійкості, захисту і зручності використання.  Ця тема включає, крім іншого, архітектуру кіберфізичних систем, базові стандарти зв’язку (Zigbee), міжплатформне програмне забезпечення, сервіс-орієнтовану архітектуру, інструменти, що підтримують контроль в реальному часі, і застосування реальних прикладів (енергосистема, ядерна установка, IoT, SCADA). |
|  | Посилення захисту системи | У цій темі розглядається захист системи шляхом пошуку та усунення ризиків. Це може включати посилення або забезпечення захисту конфігурації системи, програмного забезпечення, прошивок і додатків.  Ця тема включає, крім іншого, виявлення ризиків, загроз і вразливостей в часто використовуваних системах (операційних системах, системах баз даних, мереж); визначення та адміністрування процедур і практик для захисту від загроз; підсилення захисту за допомогою відповідних інструментів (брандмауер, антивірус, IDS, пастки для хакерів). |
|  | Доступність | Для нормальної роботи системи потрібно, щоб всі системи підтримували цільові рівні доступності, відновлюючи їх поточний стан після збою шляхом резервування, резервного копіювання і відновлення.  Ця тема включає, крім іншого, визначення ключових ресурсів і адміністрування інструментів для перевірки резервного копіювання і відновлення системи. |
| Планування у сфері кібербезпеки |  |  |
|  | Стратегічне планування | Процес визначення стратегії або напряму у сфері кібербезпеки організації і визначення необхідних дій і ресурсів, які повинні бути виділені для реалізації такої стратегії.  Ця тема охоплює такі поняття, як визначення поточного стану організації; виконання аналізу сильних і слабких сторін, можливостей та загроз (SWOT); розробка стратегії, яка відповідає місії, цінностям і баченню організації; визначення довгострокових цілей; вибір ключових показників ефективності (KPI) для відстеження прогресу; виділення необхідного бюджету; розгортання стратегії для організації; оновлення та адаптація щорічно. |
| [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, «Захист людини», стор. 44 і «Захист суспільства», стор. 62*] | Оперативне і тактичне управління | Здатність організації надійно управляти організаційно-технічною інфраструктурою.  Ця тема включає обговорення захисту даних і конфіденційності за замовчуванням і проектування, а також охоплює основні поняття, проблеми і методи для проведення ефективних і результативних операцій. Особлива увага приділяється вдосконаленню процесів та управлінню ланцюжками поставок. Тема включає стратегію операцій; тактичні стратегії; проектування продукту і сервісів; розробку процесів і аналіз; планування ресурсів; системи бережливого виробництва; управління матеріалами і запасами; управління якістю і методикою «Шість Сигм»; управління проектами; управління ланцюгами поставок. |
| Безперервність бізнесу, аварійне відновлення і управління інцидентами |  | Опис ролі аварійного відновлення (DR) в забезпеченні безперервності бізнесу (BC). Планування ВС включає в себе планування на випадок непередбачених обставин, реагування на інциденти, реагування на надзвичайні ситуації, дії організації щодо резервного копіювання і відновлення для забезпечення доступності критично важливих ресурсів під час надзвичайної ситуації, аварійне відновлення відноситься до відновлення системи в разі збою. Безперервність діяльності організацій після значних подій також є одним з компонентів теми.  Ця тема включає в себе створення та використання планів IR/DR/BP BC, організацію планів, можливість перегляду/переписування планів, вивчення планів санації, можливості для студентів написати плани на основі конкретних випадків або фактичні плани, щоб отримати певний досвід. |
|  | Реагування на інциденти | Реагування на інциденти (IR) відноситься до дій, вжитих вищим керівництвом для визначення процесів і процедур організації для прогнозування, виявлення і пом’якшення наслідків інциденту.  Ця тема включає в себе створення та використання планів IR, організацію планів, приводів для перегляду / переписування планів і вивчення планів санації. Студентам слід надати можливість написати плани на основі конкретних випадків або фактичні плани, щоб отримати певний досвід. |
|  | Аварійне відновлення | Аварійне відновлення (DR) відноситься до дій, вжитих вищим керівництвом, щоб визначити дії організації з підготовки і відновлення після аварії. Зокрема, DR відноситься до відновлення систем в разі аварії.  Ця тема включає в себе створення та використання планів аварійного відновлення, організацію планів, приводів для перегляду / переписування планів, а також вивчення планів санації. Студентам слід надати можливість написати плани на основі конкретних випадків або фактичні плани, щоб отримати певний досвід. |
|  | Безперервність бізнесу | Безперервність бізнесу відноситься до дій, вжитих вищим керівництвом, щоб визначити дії організації, якщо аварія робить основне робоче місце організації непридатним для використання. Планування безперервності бізнесу (ВС) включає в себе планування на випадок непередбачених обставин, реагування на інциденти, реагування на надзвичайні ситуації і дії організації щодо резервного копіювання і відновлення для забезпечення наявності критичних ресурсів під час надзвичайної ситуації. Безперервність діяльності організацій після значних подій також є одним з компонентів.  Навчальні плани мають включати в себе створення і використання планів ВС, організацію планів, можливість перегляду / переписування планів, а також вивчення планів санації. Студентам слід надати можливість написати плани на основі конкретних випадків або фактичні плани, щоб отримати певний досвід. |
| Управління програмами з забезпечення безпеки |  |  |
|  | Управління проектами | Управління проектами є застосування знань, навичок, інструментів і методів для проектної діяльності відповідно до вимог проекту.  Ця тема включає інтеграцію проекту; управління предметною областю проекту; управління часом і витратами в рамках проекту; управління якістю; людські ресурси; комунікації; управління ризиками; управління закупівлями. |
|  | Управління ресурсами | Управління ресурсами - це ефективне і дієве розміщення і розподіл ресурсів організації, коли і де вони необхідні. Такі ресурси можуть включати фінансові ресурси, інвентарні запаси, людські ресурси, виробничі ресурси чи інформаційні технології.  У цій темі описуються і розвиваються сучасні методи управління ресурсами, зокрема в контексті проектів, характерних для кібербезпеки. |
|  | Метрики безпеки | Метрики безпеки, часто описувані як заходи, є ефективними інструментами для визначення ефективності компонентів їх програм з забезпечення безпеки і управління діями, що вживаються для поліпшення програм з забезпечення безпеки.  У цій темі описуються елементи метрик безпеки, а також їх проектування, розробка, перевірка і організація. Використання метрик в різних контекстах повинно включати, наприклад:   * Використання метрик безпеки при прийнятті рішень, * Використання метрик безпеки в стратегічному, тактичному і оперативному плануванні; * Використання метрик безпеки при оцінці, перевірці і виконанні програм з забезпечення безпеки. |
|  | Забезпечення якості і контроль якості | Забезпечення якості (QA) і контроль якості (QC) є методами, використовуваними для запобігання помилок, які можуть вплинути на характер продукту, такого як система програмного забезпечення; контроль, як правило, відноситься до методів, що використовуються для підвищення якості цих систем.  Ця тема пояснює і розвиває поточну практику QA / QC, особливо в контексті проектів, типових для кібербезпеки. |
| Кадрова безпека |  |  |
| [*Див. для отримання додаткової інформації також галузь знань «Захист людини», стор. 44*] | Обізнаність про безпеку, навчання та освіта | Ця тема охоплює запобігання та / або належне використання невизначеності, страху і сумнівів (FUD) в якості інструменту для усвідомлення.  Ця тема включає фізичну безпеку; безпека робочого столу; безпека паролів; бездротові мережі; фішинг у сфері безпеки; спільне використання файлів і авторські права; перегляд даних; шифрування; інсайдерська загроза; міжнародні поїздки; соціальні мережі і соціальна інженерія. |
|  | Практики найму персоналу | Такі практики регулюються стратегіями, що використовуються організаціями, і застосовуються для найму і навчання персоналу організації.  Ця тема включає в себе основні принципи, студенти повинні отримати досвід за допомогою перегляду вигаданих резюме, перевірок вигаданого оточення, методів розігрування вигаданих ролей при проведенні інтерв’ю, результатів аналізу відбитків пальців, а також перевірки фінансового положення. |
|  | Практика звільнення персоналу | Практики, керовані політиками, які використовуються організаціями для звільнення працівників організації, включаючи відновлення призначених ресурсів, видалення облікових даних і завчасне запобігання просочуванню даних.  Ця тема включає в себе основні принципи, студенти повинні отримати досвід роботи з наборами практики і моделювання. |
|  | Безпека третіх сторін | Це практика організацій з управління ризиками, що можуть виникнути з боку підрядників, консультантів і співробітників ключових ділових партнерів.  Ця тема включає в себе основні принципи, студенти повинні отримати досвід роботи з наборами практики і моделювання. |
|  | Безпека під час оцінки персоналу | Це практика організацій, пов’язана з управління періодичним оцінюванням співробітників.  Ця тема включає в себе основні принципи, студенти повинні отримати досвід роботи з наборами практики і моделювання. |
| [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, «Захист людини», стор. 44 і «Захист суспільства», стор. 62*] | Спеціальне питання про конфіденційність особистої інформації співробітників | Це практика організацій щодо захисту особистої інформації співробітників та інших зацікавлених сторін.  Ця тема включає в себе основні принципи, студенти повинні отримати досвід роботи з наборами практики і моделювання. |
| Операції з забезпечення безпеки |  | Цей розділ знань охоплює заходи з підвищення безпеки походження і відстеження компонентів системи, що поставляються із зовнішніх джерел, таких як апаратне або програмне забезпечення. |
|  | Конвергенція безпеки | Злиття управлінської підзвітності в областях корпоративної (фізичної) безпеки, корпоративного управління ризиками, комп’ютерної безпеки, безпеки мережі, таке явище як InfoSec можна було спостерігати на практиці у багатьох середніх і великих організаціях.  Ця тема включає в себе нові приклади конвергенції на практиці, які можуть послугувати для обговорення виникаючих тем в класі. |
|  | Міжнародні операційні центри з забезпечення безпеки (GSOC) | Оптимізовані процеси можуть підвищити цінність організаційних операційних центрів широкого профілю, які комбінують фізичну безпеку і кібербезпеку.  У цій темі описується, як кореляція міжнародних атак з локальними заходами відповідності іноді є необхідністю. Як напад в Малайзії впливає на бізнес-функції в Колорадо? Функції GSOC повинні мати чіткий зв’язок з виявленою атакою, а також з виявленим регіоном нападу і регіоном походження. GSOC повинні бути в змозі повністю визначити тип атаки, профіль і походження, щоб мати можливість поширювати цю інформацію в інші операційні центри безпеки. |

**4.7.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Управління ризиками |  |
|  | Опишіть управління ризиками і його роль в організації. |
|  | Опишіть методи управління ризиками для визначення та пріоритизації факторів ризику для інформаційних ресурсів і методи оцінки ризику. |
|  | Обговоріть варіанти стратегії, які використовуються для обробки ризику, і будьте готові обирати один з них, коли буде надано довідкову інформацію. |
|  | Опишіть популярні методології, що використовуються в галузі для управління ризиками. |
| Управління і політика |  |
|  | Обговоріть важливість, переваги та бажані результати управління кібербезпекою та способи реалізації такої програми. |
|  | Опишіть політику інформаційної безпеки та її роль в успішній програмі з забезпечення інформаційної безпеки. |
|  | Опишіть основні типи політики інформаційної безпеки та основні компоненти кожної з них. |
|  | Поясніть, що необхідно для розробки, здійснення і підтримки ефективної політики і з якими наслідками може зіткнутися організація, якщо вона цього не зробить. |
| Закони, етичні норми і їх дотримання |  |
|  | Поясніть відмінність між правом і етикою. |
|  | Опишіть, чому кодекси етичної поведінки важливі для фахівців з кібербезпеки та організацій. |
|  | Визначте важливі національні та міжнародні закони, що стосуються кібербезпеки. |
|  | Поясніть, як організації досягають відповідності національним і міжнародним законам і правилам, а також галузевим стандартам. |
| Стратегія і планування |  |
|  | Поясніть, що таке стратегічне організаційне планування у сфері кібербезпеки та його зв’язок із загальноорганізаційним та ІТ-стратегічним плануванням. |
|  | Визначте ключові зацікавлені сторони організації та їх ролі. |
|  | Опишіть основні компоненти планування впровадження системи забезпечення кібербезпеки. |

**4.8 Галузь знань: Захист суспільства**

Галузь знань з захисту суспільства зосереджена на аспектах кібербезпеки, які впливають на суспільство в цілому на кращу або гіршу сторону. Кіберзлочинність, право, етика, політика, конфіденційність і їх зв’язки є ключовими поняттями цієї галузі знань. Загроза кіберзлочинності в міжнародному суспільстві неймовірно серйозна і продовжує зростати. Закони, етика і політика мають життєво важливе значення для забезпечення безпеки корпоративних і урядових секретів і ресурсів, а також для захисту приватного життя і особистих даних.

**4.8.1 Розділи знань і теми**

У наступній таблиці перераховані основні поняття, розділи знань і теми галузі знань з захисту суспільства.

|  |  |  |
| --- | --- | --- |
| **ЗАХИСТ СУСПІЛЬСТВА** | | |
| **Основні поняття**  - Кіберзлочинність,  - Кіберправо,  - Кібер-етика,  - Кіберполітика,  - Конфіденційність. | | |
| Розділ знань | Теми | Опис/рекомендації щодо викладання |
| Кіберзлочинність |  | Цей розділ знань спрямований на те, щоб надати студентам розуміння сфери дії, збитків і правового середовища, пов’язаних з кібер-крадіжкою інтелектуальної власності. Включає як національні, так і міжнародні середовища. Студенти повинні мати чітке уявлення про основні закони про права власності і вміти допомагати іншим орієнтуватися в складному правовому та етичному світі прав інтелектуальної власності. |
|  | Діяльність кіберзлочинців | Діяльність, яка спрямована на атаку окремих або корпоративних обчислювальних пристроїв або комп’ютерну інфраструктуру для виконання шкідливих дій, таких як поширення вірусів, крадіжка даних, крадіжка особистості. |
|  | Кібертероризм | Діяльність в кіберпросторі, спрямована на породження суспільного страху і невизначеності. |
|  | Розслідування кіберзлочинів | Методи розслідування кібератак злочинців, кіберзлочинних організацій, зарубіжних зловмисників і терористів. |
|  | Економіка кіберзлочинів | * Ризики вчинення кіберзлочину занадто низькі, в той час як вигоди занадто високі, * Використання (не відстежуваних) криптовалют при здійсненні кіберзлочинів в Інтернеті і в даркнеті (біткойн). |
| Кіберправо  [*Див. для отримання додаткової інформації також галузь знань «Захист організації», стор. 51*] |  | Мета цього розділу знань дати студентам загальне уявлення про сучасне правове середовище, пов’язане з кіберпростором. Включає як національне, так і міжнародне право, а також застосування юрисдикційних кордонів у кібернетичних судових справах. Студенти повинні мати чітке уявлення про чинне законодавство і значний досвід у формуванні цих правових інструментів. |
|  | Конституційні засади кіберправа | Ця тема включає наступне:   * Виконавча влада, * Законодавча влада, * Перша поправка, * Четверта поправка, * Десята поправка. |
|  | Право інтелектуальної власності, пов’язане з кібербезпекою | Ця тема включає наступне:   * Сфера дії, збитки і правове середовище, пов’язані з розкраданням інтелектуальної власності в кіберпросторі, * Зміст буде визначатися конкретною країною. У США, розділ 1201 Закону «Про авторське право в цифрову епоху», * Протидія обходу законів - Закон «Про авторське право в цифрову епоху» (DMCA 1201). |
| [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, «Захист людини», стор. 44 і «Захист організації», стор. 51*] | Закони про конфіденційність | Ця тема включає наступне:   * Закони, що регулюють конфіденційність в Інтернеті, * Закони, що регулюють конфіденційність в соціальних мережах, * Закони про спостереження за допомогою електронних засобів, такі як закон про прослуховування, закон про зберігання повідомлень і закон про реєстратори телефонних дзвінків. |
|  | Закони про захист даних | Ця тема включає наступне:   * Розділ 5 Закону «Про створення Федеральної Торгової Комісії США», * Закони штатів про захист даних, * Закони штатів про повідомлення про просочування даних, * Закон «Про спадкоємність страхування та звітність в галузі охорони здоров’я» (HIPAA), * Закон Гремма Ліча Блайлі (GLBA), * Обмін інформацією через US-CERT, закон про кібербезпеку 2015 року. |
|  | Закони про злом комп’ютерів | Ця тема включає наступне:   * Федеральні закони США про комп’ютерні злочини, такі як Закон «Про комп’ютерне шахрайство та зловживання». Більшість комп’ютерних хакерських злочинів переслідуються за Законом «Про комп’ютерне шахрайство і зловживання» в США. * Міжнародні рамки і співпраця, необхідні для переслідування іноземних хакерів. |
|  | Цифрові докази | Ця тема включає наступне:   * Збір криміналістично обґрунтованих цифрових доказів, * Збереження порядку передачі і зберігання доказів. |
|  | Цифрові контракти | Ця тема включає наступне:   * Відмінність між угодою, що укладається шляхом перегляду веб-сайту (browse-wrap), ліцензією на користування програмного забезпечення (click-wrap) і угодою, що знаходиться в середині упаковки (shrink-wrap). * Закон «Про електронні підписи в міжнародному та національному комерційному обороті» (ESGICA) 2000 року; цифрові контракти та електронні підписи є настільки ж законними та мають позовну силу, як і традиційні паперові контракти, підписані чорнилом. |
|  | Багатонаціональні конвенції (угоди) | Ця тема охоплює юрисдикційні обмеження багатонаціональних угод.  Приклади: Будапештська Конвенція про кіберзлочинність і Угода країн великої 7 про кібербезпеку фінансових установ. |
| [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, «Захист людини», стор. 44 і «Захист організації», стор. 51*] | Транскордонні закони про конфіденційність і безпеку даних | Вимоги Загального регламенту захисту даних (GDPR). Угода про правила обміну конфіденційною інформацією між такими країнами, як США і Великобританія, що дозволяє передачу персональних даних. |
| Кібер-етика  [*Див. для отримання додаткової інформації також галузі знань «Захист організації», стор. 51 і «Захист програмного забезпечення», стор. 23*] |  | Цей розділ знань покликаний дати студентам основу для розуміння і застосування моделей моральних міркувань для вирішення поточних і виникаючих етичних дилем на індивідуальному та груповому (професійному) рівні. Він також допомагає студентам зрозуміти, чи є етика в обчислювальних технологіях унікальною проблемою або частиною більш масштабного явища, і допомагає студентам обміркувати, як культура і правові рамки їхньої країни впливають на розуміння і реалізацію етики в їхньому суспільстві. |
|  | Визначення етики | У рамках цієї теми слід навчитися:   * Порівнювати і протиставити основні етичні позиції, включаючи доброчесну етику, утилітарну етику і деонтологічну етику. * Застосовувати три різні етичні позиції при осмисленні етичних наслідків конкретної проблеми або дії. |
|  | Професійна етика і кодекси поведінки | Ця тема охоплює:   * Основні професійні товариства, такі як ACM, IEEE-CS, AIS і (ISC)2, * Професійна відповідальність, * Етична відповідальність щодо спостереження. |
|  | Етика і справедливість / різноманітність | У межах цієї теми слід навчитися:   * Описувати, яким чином алгоритми прийняття рішень можуть надмірно або неповністю представляти інтереси груп більшості і меншості в суспільстві, * Аналізувати, яким чином алгоритми можуть неявно включати соціальні, гендерні та класові упередження. |
|  | Етика і право | У межах цієї теми слід навчитися:   * Розуміти, що дотримання етичних норм і правові кодекси не завжди можуть точно співпадати, * Дотримання етичних норм може розглядатися як універсальне явище, в той час як закони можуть бути національними або регіональними (наприклад, Європейський Союз), * Закони можуть розвиватися, але етичні цінності можна охарактеризувати як незмінні. |
|  | Автономія / етика роботів | У рамках цієї теми слід навчитися:   * Визначати автономний процес прийняття рішень, * Давати визначення штучного інтелекту і описувати етичні дилеми, пов’язані з використанням або працевлаштуванням штучного інтелекту (AI), * Описувати законодавчі досягнення, що визначають особистість і цифрову особистість, * Характеризувати конфлікт, створюваний правовими поняттями відповідальності і використанням некерованих людиною або автономних програм прийняття рішень. |
|  | Етика і конфлікти | Ця тема включає наступне:   * Принципи справедливої війни в кіберпросторі у зв’язку з початком конфлікту, поведінкою у конфлікті, припиненням конфлікту/постконфліктною ситуацією; * Етичні проблеми, що виникають при здійсненні кібершпіонажу; * Порушення норм і правил стосовно кібертероризму. |
|  | Етика злому | Ця тема включає наступне:   * Етичне тестування на проникнення проти неетичного злому, * Етичні принципи і умови злому, * Відмінності між зломом з метою завдавання шкоди, хактивізмом, зломом зі злочинними цілями і військовими діями. |
|  | Етичні рамки і нормативні теорії | Загальні етичні рамки і нормативні теорії, пов’язані з кібербезпекою з індивідуальної та соціальної точок зору. |
| Кіберполітика  [*Див. для отримання додаткової інформації також галузь знань «Захист організації», стор. 51*] |  | Цей розділ знань з кіберполітики покликаний допомогти студентам зрозуміти і проаналізувати кібернетичні проблеми, оскільки вони пов’язані з національними інтересами в цілому і з національною політикою (і національною безпекою) зокрема. Студенти повинні отримати уявлення про питання, що відносяться до використання кіберпростору як знаряддя війни, і розрізняти використання кіберпростору в якості такого інструменту і можливість початку кібервійни. Студентам буде надана можливість відповісти на питання про те, як про використання кіберпростору може бути повідомлено іншим країнам, а також про проблеми, пов’язані з його стримуванням. Студенти також повинні розуміти історичні тенденції, які зробили кіберпростір важливим для національної політики, і розвиток структури національної кіберполітики. Очікується, що студенти продемонструють оригінальне мислення про те, як кіберпростір впливає на національні інтереси, в тому числі економічні, і політичні наслідки, пов’язані з використанням кіберпростору, для національної політики. |
|  | Міжнародна кіберполітика | Ця тема включає наступне:   * Проблеми міжнародної кіберполітики, * Закон про контроль міжнародної кіберполітики 2015 року, * Стратегія Держдепартаменту в галузі міжнародної кіберполітики. |
|  | Кіберполітика США | Ця тема включає наступне:   * Закон про вдосконалення інформаційної безпеки федерального уряду, оновлення політики і інструкцій федерального уряду в галузі кібербезпеки, * Зв’язок з найважливішою інфраструктурою країни, * Управління ризиками на національному рівні. |
|  | Світове значення | Ця тема охоплює:   * Вплив кібербезпеки на міжнародну систему в цілому і на міжнародну безпеку зокрема. * Як кіберпростір став і залишиться інструментом влади і як ця сила може змінити баланс сил між сильними та слабкими країнами. * Світове регулювання кіберпростору. Також розглянуто можливості розвитку нормативної поведінки, пов’язаної з використанням кіберпростору. * Вплив кіберпростору на світову економіку. |
|  | Політика кібербезпеки та національної безпеки | Ця тема охоплює:   * Як країна визначає свою політику кібербезпеки, доктрину і відповідальність за її здійснення, включаючи національну політику кібербезпеки, структуру, попередження і концепції, а також примушення і погрози, * Повідомлення, що стосуються кібербезпеки країни; як повідомляють про свої наміри привернути увагу і співпрацювати з іншою країною. |
|  | Вплив кібербезпеки для економіки країни | Ця тема охоплює:   * Вартість кібербезпеки для країни, * Переваги і недоліки кібербезпеки для країни, * Інвестиції на захист держави від кіберзагроз і кібератак. |
|  | Нові примикання до дипломатії | Ця тема включає наступне:   * «Витончений танець» кібер-дипломатії, * Аспекти кібербезпеки, які стали частиною відносин між країнами, включаючи прихований збір інформації поряд з практикою дипломатії і приховане застосування кібервійськ у кіберпросторі та фізичному просторі. |
| Конфіденційність  [*Див. для отримання додаткової інформації також галузі знань «Захист даних», стор. 16, «Захист людини», стор. 44 і «Захист організації», стор. 51*] |  | Цей розділ знань призначений для того, щоб надати студентам розуміння конфіденційності та пов’язаних з нею проблем. Студенти повинні розуміти компроміси обміну і захисту конфіденційної інформації, а також те, як внутрішні та міжнародні права на недоторканність приватного життя впливають на відповідальність компанії за збір, зберігання та обробку персональних даних. Студенти отримають уявлення про технології підвищення конфіденційності і додатки системи безпеки, які можуть включати в себе концепції належного використання, а також захисту інформації. |
|  | Визначення конфіденційності | У рамках цієї теми слід навчитися:   * Застосовувати робоче визначення конфіденційності, * Визначати різні цілі конфіденційності, наприклад конфіденційність повідомлень і конфіденційність метаданих, * Визначати компроміси конфіденційності - підвищення рівня конфіденційності може мати ризики (наприклад, використання Tor може зробити когось мішенню для посилення урядового контролю в деяких частинах світу). |
|  | Права на недоторканість приватного життя | У рамках цієї теми слід навчитися:   * Описувати умови інформованої згоди щодо збору персональних даних та обміну ними, * Визнавати національні права на недоторканність приватного життя за наявності прав на недоторканність приватного життя, * Демонструвати обізнаність з дискусією з питання про універсальне право людини на недоторканність приватного життя. |
|  | Захист конфіденційності | У рамках цієї теми слід навчитися:   * Перераховувати заходи кібер-гігієни для захисту недоторканності приватного життя, * Перераховувати технології підвищення рівня конфіденційності та їх використання, а також властивості, які вони надають і не надають (наприклад, Tor, шифрування), * Описувати умови етичного і законного використання технологій, що підвищують рівень конфіденційність, * Описувати заходи з проведення оцінки впливу на конфіденційність, * Описувати роль довірчого керуючого даними, * Описувати законодавство, пов’язане з практикою локалізації даних, * Демонструвати розуміння різниці між правами на недоторканність приватного життя і можливостями підвищення рівня конфіденційності - операціоналізація приватного життя, * Обговорювати динамічний вплив метаданих і великих обсягів даних на конфіденційність. |
|  | Норми конфіденційності та відношення до неї | Ця тема включає наступне:   * Теорія і моделі обчислення конфіденційності, * Культурні відмінності при існуванні норм і кордонів приватного життя. |
|  | Порушення конфіденційності | У цій темі розглядається роль корпорацій в захисті даних і вирішенні проблем, пов’язаних з порушенням конфіденційності даних. |
|  | Конфіденційність в суспільствах | Ця тема включає наступне:   * Права на недоторканність приватного життя і загрози недоторканності приватного життя, пов’язані з громадськими діячами, * Диференційоване спостереження і пов’язані з ним ризики; проблеми «розумних» міст, * Матриця шкоди, пов’язаної зі спостереженням в цілях забезпечення кібербезпеки. |

**4.8.2 Основні поняття і цілі навчання**

Студенти повинні продемонструвати знання кожного з основних понять шляхом досягнення цілей навчання. Як правило, цілі навчання знаходяться в межах елементів *розуміння* і *застосування* переглянутої таксономії Блума (<http://ccecc.acm.org/assessment/blooms>).

|  |  |
| --- | --- |
| **Основні поняття** | **Цілі навчання** |
| Кіберзлочинність |  |
|  | Обговоріть різні мотиви дій кіберзлочинців |
|  | Узагальніть терористичну діяльність в кіберпросторі, спрямовану на породження суспільного страху і невпевненості. |
|  | Опишіть методи розслідування як внутрішніх, так і міжнародних злочинів |
|  | Поясніть, чому збереження порядку передачі і зберігання цифрових доказів необхідно для переслідування кіберзлочинців. |
| Кіберправо |  |
|  | Опишіть конституційні засади кіберправа. |
|  | Опишіть міжнародні закони щодо захисту даних і злому комп’ютерів. |
|  | Тлумачення законів про інтелектуальну власність, що стосуються безпеки. |
|  | Узагальніть закони, що регулюють конфіденційність в Інтернеті. |
| Кібер-етика |  |
|  | Роз’ясніть, що таке доброчесна етика, утилітарна етика і деонтологічна етика. |
|  | Перефразуйте професійну етику і кодекси поведінки відомих професійних спільнот, таких як ACM, IEEE-CS, AIS і (ISC)2. |
|  | Опишіть способи, за яких алгоритми прийняття рішень можуть надмірно представляти або неповністю представляти інтереси більшості і меншості в суспільстві. |
| Кіберполітика |  |
|  | Опишіть основні позиції в галузі міжнародної політики та їх вплив на організації та окремих осіб. |
|  | Узагальніть національну політику в галузі кібербезпеки щодо захисту конфіденційної інформації та захисту критичної інфраструктури. |
|  | Поясніть світовий вплив кібербезпеки на культуру, включаючи такі області, як економіка, соціальні питання, політика та закони. |
| Конфіденційність |  |
|  | Опишіть концепцію конфіденційності, включаючи суспільне визначення того, що являє собою особиста інформація, і компроміси між конфіденційністю і безпекою. |
|  | Коротко охарактеризуйте компроміс між правами на недоторканність приватного життя індивіда і потребами суспільства. |
|  | Опишіть загальні методи і технології, використовувані для захисту приватного життя. |

**Глава 5: Галузеві перспективи кібербезпеки**

Галузь кібербезпеки знаходиться на стадії становлення і відчуває дедалі більші труднощі через відсутність структурованої дисципліни, потреба в якій визнається у всій галузі.

У той час як галузь кібербезпеки зросла за останні десятиліття, визначення кібербезпеки як самостійної дисципліни часто ігнорується або упускається з виду як важливий фактор успіху для створення і розвитку професійних кадрів, необхідних для урядових структур і промислових підприємств для забезпечення безпеки їхніх систем. На сьогоднішній день одностайною позицією є те, що рішення проблем кібербезпеки має бути пріоритетом як для держав, так і для бізнесу, а потреба у структурованій дисципліні очевидна.

У той час як програми, спрямовані на підготовку фахівців з кібербезпеки увінчалися певним успіхом, загальний брак фахівців, який за оцінками досягне 1,8 мільйона в 2022 році ((ISC)2, 2017 р.), продовжує зростати[[13]](#footnote-13).

На жаль, хоча і існують вільні робочі місця, знайти кваліфікованих фахівців часто буває важко. Студенти, які навчалися за технічними спеціальностями, такими як «Інформаційні технології» або «Інформатика», часто не мають конкретних знань і навичок з кібербезпеки, необхідних для роботи в урядових організаціях або на промислових підприємствах. Студенти, які навчалися за нетехнічними спеціальностями, часто отримують тільки поверхневі знання про основні поняття кібербезпеки і, таким чином, не мають глибинного розуміння понять кібербезпеки, необхідних для застосування їхніх знань і навичок у роботі.

**5.1 Комплекс техніко-ділових навичок**

Багато рішень проблеми кібербезпеки носять технічний характер, але вони також вимагають, щоб окремі особи і організації реалізовували політику та програмні заходи для забезпечення належного функціонування призначених систем управління. В рамках дисципліни «Кібербезпека» існує цілий ряд необхідних навичок, починаючи від технічних (таких, як криптографія та захист мереж) до управлінських (таких, як планування, розробка політики та дотримання нормативних вимог). Незалежно від положення серед фахівців з кібербезпеки, кожен випускник програми за напрямком «Кібербезпека» буде потребувати поєднання навичок з різних сфер цього безперервного ряду і повинен володіти як технічними навичками, так і діловим хистом, щоб ефективно брати участь у вирішенні проблем, аналізі та управлінні проектами для реалізації рішень з кібербезпеки.

Нетехнічні (іноді звані «комунікативними») навички життєво важливі для успіху професіоналів у галузі кібербезпеки. Здатність працювати в команді, роз’яснювати технічні теми нетехнічним аудиторіям, успішно сперечатися про розподіл ресурсів, відточувати ситуаційну обізнаність і діяти в рамках розрізнених організаційних культур - ось лише деякі з таких навичок. Поміж інших організацій, Рада директорів з людського капіталу США (CHCO) розробила список нетехнічних професійних якостей і навичок, що мають відношення до фахівців з кібербезпеки.

Список включає в себе наступне: відповідальність, увага до деталей, стійкість, управління конфліктами, розсудливість, усне і письмове спілкування і командна робота. Повний перелік професійних якостей і навичок доступний у Зразковому прикладі професійних якостей і навичок фахівців з кібербезпеки[[14]](#footnote-14). Такі професійні асоціації, як (ISC)2, ISACA і CompTIA, також надають рекомендації щодо нетехнічних навичок, необхідних для фахівців з кібербезпеки.

**5.2 Кар’єрні можливості**

Оскільки студенти готуються до будування кар’єри у майбутньому, важливим чинником є їх здатність перейти від академічного середовища до будування кар’єри в корпорації, організації, навчальному закладі або навіть підприємницькому середовищі. Можна представити, яким важким може бути такий перехід, якщо людина не отримала належного поєднання технічних навиків, пов’язаних з кібербезпекою, і навичок спілкування під час свого навчання. Багато співавторів цього посібника вказали на нагальну необхідність задоволення потреб у робочій силі в галузі кібербезпеки в майбутні роки, яка виникає як в їх компаніях, так і в більш широкому діловому співтоваристві.

Адаптивність, тобто здатність легко пристосовуватися до різних умов середовища і ситуаційного контексту, є особливо важливою рисою для людей, що працюють в галузі кібербезпеки. Фахівці з кібербезпеки знайдуть можливість вивчати нові технології і приймати зміни, які будуть мати велике значення в найближчі роки. Джорджія Нуджент стверджує: «Це жахлива іронія, що в той самий момент, коли світ став більш складним, ми заохочуємо наших молодих людей бути вузькоспеціалізованими в одній галузі. Ми робимо ведмежу послугу молодим людям, кажучи їм, що життя - це прямий шлях. Гуманітарні науки, як і раніше актуальні, тому що вони навчають студентів бути гнучкими і адаптуватися до мінливих обставин.»[[[15]](#footnote-15)](#bookmark14) Індустрія кібербезпеки історично приваблювала людей, які процвітають в цьому середовищі постійних змін.

На додаток до акценту на галузь і отримання безцінного досвіду роботи під час навчання в навчальному закладі, важливо, щоб студенти, які згодом мають закінчити навчання, готувалися до співбесід, структуруючи свої резюме в форматі, який підкреслює їхню підготовку у галузі інформаційних технологій. Що відрізняє резюме технічного фахівця від стандартного, так це акцент на таких атрибутах, як конкретні технічні навички та галузеві сертифікати. Monster.com, провідний сайт з працевлаштування, є хорошим джерелом для прикладів того, як створити резюме технічного фахівця.[[[16]](#footnote-16)](#bookmark15)

Уміння успішно пройти співбесіду є навичкою, необхідною для будування кар’єри і яку студентам важливо практикувати і освоїти в ході їхнього навчання. Це так само важливо, як вивчення основних технічних предметів. Якщо студенти не в змозі впоратися з суворістю співбесід, їх середній академічний бал і різні наукові досягнення не допоможуть в досягненні бажаної мети при отриманні освіти у галузі кібербезпеки – закінчити навчання і отримати роботу, яка сприятиме становленню як фахівця і кар’єрному зростанню.

Консультативна рада з кібербезпеки може допомогти в тому, щоб навчальні програми забезпечували студентів важливими зв’язками і контактами в рамках індустрії кібербезпеки у більш широкому значенні і конкретними варіантами працевлаштування в галузі кібербезпеки, які допоможуть їм успішно впоратися зі співбесідою. Часто консультативні ради виступають в якості наставників для студентів, даючи їм цінні відгуки і коментарі щодо їхніх резюме та підготовки. Вони часто допомагають і заохочують студентів працювати на стажуваннях, цінність яких також є темою для обговорення. Крім того, важливість нетехнічних навичок і вміння ладнати в колективі також є необхідними компонентами для налагодження корисних професійних контактів. Для просування своєї кар’єри в майбутньому, вміння спілкуватися і знаходити кар’єрні можливості стане дуже важливою навичкою.

**5.3 Зв’язок навчальної програми з кібербезпеки з професійною практикою**

Практика з кібербезпеки передбачає поєднання знань і навичок, необхідних для роботи на місцях. Практика є критично важливим аспектом в освіті в галузі кібербезпеки. Модель мислення CSEC пов’язує навчальну програму з професійною практикою за допомогою використання областей застосування. Області застосування забезпечують організаційну структуру для об’єднання змісту навчальних програм, професійного розвитку та можливостей навчання, а також отримання професійних сертифікатів.

**5.3.1 Області застосування**

Області застосування служать в якості організаційної структури для визначення рівнів компетентності для кожної практики. Області застосування допомагають визначити глибину охоплення, необхідну для кожного основоположного поняття. Крім того, області застосування забезпечують зв’язок між моделлю мислення і конкретним планом підготовки фахівців.

До сімох областей застосування входять:

• **Державна політика**. Виконавчі керівники на рівні генерального директора або ради директорів; законодавці, які приймуть закони, що впливають на розробку, впровадження та використання інформаційних технологій; регулюючі органи, які будуть регулювати ці питання; та інші державні та приватні посадові особи, які розроблятимуть фактичну державну політику. Ці люди повинні розуміти, як ці закони, нормативні акти та вимоги впливають на використання систем, як люди взаємодіють з ними і з регулюючими органами, як проводиться перевірка дотримання і які ризики державна політика контролює і вводить. Вони повинні розуміти основи проектування, оскільки проектування системи і процес, у якому організація використовує її, впливає на спосіб реалізації і тестування відповідності. Це призводить до необхідності розуміти, що обчислювальна система може і (що більш важливо) не може робити. Це також означає, що вони повинні розуміти вартість забезпечення безпеки з точки зору бюджету та людських ресурсів.

• **Закупівля**. Ті, хто закуповує інформаційні технології і наймає людей, які будуть з ними працювати, повинні розуміти, яким чином системи і наймані працівники вписуються в цілі організації в цілому і конкретні цілі проектів, для яких здійснюються закупівлі і найм персоналу. Це вимагає розуміння як безперервності бізнесу, так і управління ризиками, що дозволяє вибирати технології і людей для мінімізації ризиків, максимального спрощення управління ризиками або (в ідеалі) і для того, і для іншого. Наслідком цього є знання того, що потрібно від людей, систем, інфраструктури, процедур і процесів для забезпечення бажаного рівня і гарантії безпеки.

• **Управління**. Управління відноситься як до систем, так і до співробітників в організації певного типу. Як внутрішня політика, так і зовнішня політика (положення, закони тощо) впливають на управління. Керівники повинні розуміти питання дотримання нормативних вимог і забезпечення безперервності діяльності, з тим щоб системи і співробітники, якими вони управляють, відповідали потребам організації та урядових і інших регулюючих органів. Оскільки вони повинні гарантувати, що люди, які використовують їх системи, уповноважені це робити, і повинні знати, ким ці люди є, їм слід добре розбиратися в управлінні ідентифікацією та авторизацією. Зміни в системах вимагають, щоб вони розуміли цілі тестування і те, чи відповідають тести цим цілям. Нарешті, вони повинні бути готові боротися з наслідками атак, розуміючи, як керувати інцидентами і як інцидент вплине на організацію. Таким чином, вони повинні мати загальне уявлення про управління інцидентами, так і про відновлення після аварій.

• **Дослідження**. Дослідники в академічних колах, промисловості та уряді, які вивчають безпеку, повинні знати основи керування доступом, конфіденційності (включаючи основні принципи та використання криптографії), цілісності і доступності. Крім того, специфіка того, що вони повинні знати, залежить від галузі досліджень і будь-яких конкретних цілей цього дослідження. Наприклад, дослідник, що вивчає захист мережі, повинен розуміти, як мережі використовуються на практиці, щоб зрозуміти, як їх робота впливає на параметри дослідження; ймовірно, немає необхідності розуміти доказ теореми HRU (Харрісона-Руззо-Ульмана) і пов’язані з нею результати. Але той, хто вивчає основні аспекти (такі як нерозв’язності), повинен знати теорему HRU і пов’язані з нею результати, а не подробиці мережевих операцій.

• **Розробка програмного забезпечення**. Програмне забезпечення має відповідати вимогам, які часто контролюються законами, нормативними актами, бізнес-планами та організаційними факторами. Розробники мають переконатися, що їхнє програмне забезпечення спроектоване для задоволення цих вимог, або вимоги є змінами, які програмне забезпечення може задовольнити. Потім реалізації повинні відповідати проекту і бути надійними (безпечне програмування), що включає в себе коректну обробку винятків і помилок. Це включає в себе врахування середовища, в якому буде працювати програмне забезпечення. Вони повинні знати, як підтвердити свої вимоги шляхом тестування програмного забезпечення. Нарешті, вони повинні бути в змозі встановити середовище, в якому програмне забезпечення буде працювати, відповідного до того, що припускає проектування і реалізація; і якщо це не може бути зроблено, вони повинні документувати такі факти у своїх інструкціях зі встановлення, і (в ідеалі) відображати відповідні повідомлення під час інсталяції програмного забезпечення.

• **Операції з забезпечення інформаційної безпеки**. Аналогічним чином, операції повинні забезпечувати безпеку системи. Оскільки безпека визначається набором вимог, системні адміністратори, співробітники служби безпеки системи і інші співробітники служби інформаційної безпеки повинні розуміти, як перетворити вимоги у процедури і конфігурації. З цією метою вони повинні вміти розробляти і впроваджувати анклави і інфраструктури, наприклад, забезпечувати правильну установку, ініціалізацію, налаштування і підключення систем управління ідентифікацією та авторизацією. Вони повинні знати, як тестувати системи, інфраструктуру і процедури, а також аналізувати отримані результати. І нарешті, оперативний персонал повинен розбиратися в обслуговуванні системи як в звичайних умовах (наприклад, при встановленні виправлень і оновленні), так і в надзвичайних умовах (наприклад, при обробці інцидентів і реагуванні на них).

• **Архітектура підприємства**. Архітектура підприємства відноситься до систем, інфраструктури, операцій і управління всіма інформаційними технологіями на підприємстві, тобто включає елементи всіх інших областей застосування.

Архітектура управляється політикою; проектування архітектури управляє закупівлями, управлінням і операціями. Архітектура також впливає на більшу частину програмного забезпечення, наприклад, те, що необхідне для роботи інфраструктури. Таким чином, архітектори підприємства повинні розумітися в таких областях застосування, як політика, закупівлі, управління та операції, а також елементах з області розробки програмного забезпечення.

**5.3.2 Навчання та сертифікація**

У галузі кібербезпеки набуття знань і підвищення кваліфікації на всіх рівнях після закінчення середньої школи відбувається як у формальних вищих навчальних закладах, так і у сфері професійного розвитку, професійної підготовки і сертифікації. Розробники навчальних програм повинні визначити і зв’язатися з організаторами навчання і тренінгів, щоб визначити можливості для співпраці.

**5.4 Основний план підготовки фахівців**

У контексті економічного середовища, ініціативи з розвитку трудових ресурсів часто обумовлені основними планами підготовки фахівців, які формують організаційну структуру для різних посадових ролей; освітою, навчанням та підвищенням вимог щодо професійного розвитку і можливостями побудувати кар’єру. У галузі кібербезпеки країни приступили до розробки основних планів підготовки фахівців з метою визначення вимог до навичок і підтримки ініціатив з розвитку трудових ресурсів. Наприклад, в США. основний план підготовки фахівців з кібербезпеки Національної ініціативи з освіти у галузі кібербезпеки (NCWF)[[17]](#footnote-17) розробляється в якості всеосяжного ресурсу для опису роботи у галузі кібербезпеки. У Сінгапурі Національна стратегія у галузі кібербезпеки закликає до підготовки і розвитку фахівців з кібербезпеки за допомогою промислово-орієнтованих навчальних програм у вищих навчальних закладах, очевидних можливостей кар’єрного зростання, а також конкретних систем оцінки компетенцій, таких як Система оцінки комптенецій з захисту даних (DPCF), розробленої для того, щоб переконатися, що посадові особи з питань захисту даних володіють необхідними навичками, компетенціями і атестаціями, необхідними для ефективного виконання обов’язків[[18]](#footnote-18). У Сполученому Королівстві Національна стратегія у галузі кібербезпеки описує, як уряд Великобританії буде підтримувати підготовку і розвиток надійних фахівців з кібербезпеки[[19]](#footnote-19). Ці національні стратегії є ілюстрацією того, як уряди в усьому світі розробляють основні плани підготовки фахівців для задоволення зростаючої потреби у фахівцях з кібербезпеки.

**5.4.1 «Дорожня карта» реалізації NCWF**

Для ефективного задоволення потреб у фахівцях навчальним закладам важливо зв’язати рекомендації щодо навчальних програм, пропоновані в цьому документі, з відповідними основними планами підготовки фахівців. Як приклад того, як це можна зробити, веб-сайт залучення спільноти (http://cybered.acm.org) надає інструкції щодо процедури складання карт та приклади «дорожніх карт», які пов’язують конкретні знання та навички посадової ролі NCWF з рекомендаціями щодо викладання CSEC. На рис. 5 показано, як «дорожні карти» зв’яжуть рекомендації щодо викладання дисципліни і основні плани підготовки фахівців.



Рис. 5. Ув’язка моделі мислення CSEC і основного плану підготовки фахівців

|  |  |
| --- | --- |
| CSEC 2017 Knowledge structure | Структура знань CSEC 2017 |
| Knowledge area | Галузь знань |
| Knowledge unit | Розділ знань |
| Topic | Тема |
| Learning outcomes | Цілі навчання |
| Content (topics and LOs are influenced by disciplinary lens and institution type) | Знання (на теми і цілі навчання впливають дисциплінарні підходи і тип закладу) |
| Category | Категорія |
| Specialty area | Галузь спеціалізації |
| Work role | Посадова роль |
| KSA | Знання, навички та вміння |

Огляд компонентів «дорожньої карти» приведено нижче на рис. 6. Перший набір зразкових «дорожніх карт» пов’язує рекомендації щодо викладання дисципліни CSEC і основоположні вимоги NCWF до знань, навичок і вмінь (KSA) шести областей спеціалізації в рамках категорії Контроль і управління (OV)[[20]](#footnote-20).

У моделі мислення CSEC основоположні знання визначаються як основні поняття кібербезпеки. Основні поняття кібербезпеки повинні вводитися на ранньому етапі і закріплюватися в рамках будь-якої програми з кібербезпеки. Основні поняття знайомлять студентів з основними концепціями і термінами кібербезпеки, середовищем загроз, загальними уразливими і основами забезпечення цілісності і безпеки інформації.

Як зазначалося вище, основні поняття чітко визначені в кожній з восьми галузей знань. Ці поняття можуть відображатися у зводі знань галузі знань як окремі розділи знань, як теми в межах конкретних розділів знань або як сукупність тем розділів знань. Основні поняття по всіх галузях знань наведені в додатку В.

Разом узяті основні поняття з усіх галузей знань включають мінімально необхідний зміст будь-якої програми з кібербезпеки.

Кожна «дорожня карта» курсу допоможе:

1. Обґрунтовувати знання та їхнє значення для конкретної ролі.

2. Визначити та описати відповідні курси та модулі курсу.

3. Намітити стратегії отримання знань в тих випадках, коли конкретні курси відсутні або недоступні в рамках певного закладу.

4. Виділити проблеми (і відповідні стратегії їх подолання), щоб слідувати запропонованому курсу дослідження.



Рис. 6. Елементи «дорожньої карти» для курсу

|  |  |
| --- | --- |
| CSEC 2017 Curricular guidance | Рекомендації щодо викладання CSEC 2017 |
| Disciplinary lens | Дисциплінарний підхід |
| Institution type | Тип закладу |
| Learning outcomes | Цілі навчання |
| Overview | Огляд |
| Relevant courses | Відповідні курси |
| Knowledge acquisition strategies | Стратегії набуття знань |
| Challenges | Проблеми |
| Ex. National cybersecurity workforce framework | Наприклад, національний план підготовки фахівців з кібербезпеки |
| Specialty area | Галузь спеціалізації |
| Knowledge, skills, abilities (KSAs) | Знання, навички та вміння |

**5.4.2 Огляд**

Обґрунтування KSA забезпечує орієнтири для студентів, що починають курс навчання, і пояснює зв’язок між знаннями і конкретною посадовою роллю.

**5.4.3 Відповідні курси**

Центральною частиною «дорожньої карти» буде визначення відповідних курсів і опис необхідного змісту курсу. Оскільки відповідні курси викладаються в вищих навчальних закладах в інтерпретації різних факультетів і в різних форматах, вкрай важливо включити в цей розділ конкретний зміст, а не просто перерахування назв курсів. Цей розділ «дорожніх карт» також включає стратегії для курсів самостійного вивчення і інші параметри.

**5.4.4 Стратегії набуття KSA**

Коледжі та університети часто мають програми та курси, які включені до декількох академічних структурних підрозділів. Крім того, деякі відповідні матеріали можуть бути доступні на заняттях, які не входять до формальної структури курсу. В результаті студентам (і їх викладачам) може бути складно визначити найбільш ефективні стратегії набуття знань. «Дорожні карти» допоможуть в цьому.

Взяті разом, елементи «дорожньої карти» забезпечують всеосяжний план для студентів і викладачів шляхом:

* Визначення змісту і глибини знань принципів кібербезпеки, необхідних для оптимального розвитку конкретних робочих ролей категорії OV.
* Розмежування знань та навчання, що базується на відповідних навиках, на звичайне (традиційне навчання) і онлайн навчання на різних ресурсах в межах і за межами університету Джорджа Вашингтона, з метою забезпечення можливості вибору, який задовольнить індивідуальні потреби студентів і очікування того, що стратегії набуття знань можуть працювати і на основі неповної зайнятості у рамках формальних програм і за ними.
* Виявлення можливостей для студентів брати участь в групових заняттях в рамках програм, які допомагають у розвитку міждисциплінарного розуміння і застосування принципів кібербезпеки.
* Використання міждисциплінарних ресурсів та залучення викладачів в рамках університету, в якому викладається низка програм, присвячених кібербезпеці, юридичній і політичній практиці, пов’язаній з кібербезпекою, і підготовці керівників/ виконавців, чия діяльність буде пов’язана з кібербезпекою.
* Визначення спеціальних можливостей практичного навчання - крім звичайного досвіду в класі, - які будуть включені в «дорожні карти»; включаючи моделювання та/або настільні вправи і спеціальні запрошені лектори (чиї лекції доступні як в Інтернеті, так і в класі). Такі можливості включатимуть в себе можливість навчатися разом з студентами технічних спеціальностей з метою поліпшення комунікації між OV і мовою різних технічних термінів - тобто, оволодіти іншою мовою і лексикою галузі кібербезпеки, так що учасники будуть краще підготовлені до ролі керівника.

**5.4.5 Проблеми**

«Дорожні карти» являють собою ідеальний план навчання. Проте реалізація «дорожніх карт» в контексті структури вищого навчального закладу, навіть якщо цей контекст безпосередньо враховувався в процесі розробки, може бути пов’язана з труднощами. У цьому розділі представлені конкретні проблеми і пропонуються стратегії їх подолання.

* Курси з відповідними знаннями викладаються у всьому навчальному закладі, і студенти не можуть легко розробити індивідуальні курси навчання
* Виконання попередніх вимог курсу може бути додатковою проблемою при переході між факультетами
* Виявлення і відстеження можливостей позакласного навчання

Членам міжнародного співтовариства рекомендується розробляти і поширювати приклади курсів, навчальних програм і планів підготовки фахівців, а також «дорожні карти» підготовки фахівців за допомогою розділу веб-сайту залучення спільноти - Сommunity engagement. Цей сайт, http://cybered.acm.org буде регулярно оновлюватися і служити основою для світового співтовариства практиків, яке пов’язує викладачів кібербезпеки і зацікавлені сторони в безперервному процесі розробки.

*[Кінець CSEC вер. 1.0]*

**Додаток B: Загальні таблиці основних понять**

|  |  |
| --- | --- |
| **Основні поняття галузі знань «Захист даних»** | **Основні поняття галузі знань «Захист програмного забезпечення»** |
| Основні поняття криптографії | Фундаментальні принципи проектування, включаючи принципи мінімальних привілеїв, відкритого проектування і абстрактної фабрики |
| Наскрізний захищений зв’язок | Вимоги безпеки та їх роль в проектуванні |
| Цифрова криміналістика | Проблеми реалізації |
| Цілісність і автентифікація даних | Статичне та динамічне тестування |
| Знищення даних | Налаштування конфігурації і виправлення |
|  | Етика, особливо при розробці, тестуванні та розкритті вразливостей |

|  |  |  |
| --- | --- | --- |
| **Основні поняття галузі знань «Захист компонентів»** | **Основні поняття галузі знань «Захист з’єднань»** | **Основні поняття галузі знань «Захист системи»** |
| Уразливості компонентів системи | Системи, архітектура, моделі і стандарти | Цілісний підхід |
| Життєвий цикл компонента | Інтерфейси фізичних компонентів | Політика забезпечення безпеки |
| Принципи безпечного проектування компонентів | Інтерфейси програмних компонентів | Автентифікація |
| Безпека управління ланцюжками поставок | Атаки на з’єднання | Керування доступом |
| Тестування безпеки | Атаки на передачі | Моніторинг |
| Зворотна розробка |  | Відновлення |
|  |  | Тестування |
|  |  | Документація |

|  |  |  |
| --- | --- | --- |
| **Основні поняття галузі знань «Захист людини»** | **Основні поняття галузі знань «Захист організації»** | **Основні поняття галузі знань «Захист суспільства»** |
| Управління ідентифікацією | Управління ризиками | Кіберзлочинність |
| Соціальна інженерія | Управління і політика | Кіберправо |
| Усвідомлення і розуміння | Закони, етика та їх дотримання | Кібер-етика |
| Конфіденційність і безпека соціальної поведінки | Стратегія і планування | Кіберполітика |
| Безпека та конфіденційність персональних даних |  | Конфіденційність |

**Додаток C: Приклади**

У цьому додатку містяться зразки навчальних планів, планів підготовки фахівців і приклади курсів.

**Зразок навчального плану**

Сукупність знань CSEC2017 забезпечує гнучкість для підтримки багатьох різних типів навчальних планів. На прикладах навчальних планів буде показано, як навчальні плани конкретних закладів охоплюють основні поняття галузей знань і деякі підгрупи розділів знань. Ці приклади будуть надані для демонстрації того, як сукупність знань може бути організована у вигляді повного навчального плану.

(Примітка: *будь ласка, видаліть виділені курсивом інструкції у ваших відповідях*.)

**Дисциплінарний підхід і тип закладу**

➔ *Виберіть дисциплінарний підхід і тип закладу, які найкраще описують вашу програму. Вкажіть основне місце розташування навчального закладу*.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Тип начального закладу** | |
| **Дисциплінарний підхід** |  | Ступінь / Тривалість програми | Країна |
| Інформатика | *(наприклад) Бакалавр / 4 роки* | *(наприклад) Сполучені Штати Америки* |
| Обчислювальна техніка |  |  |
| Програмна інженерія |  |  |
| Інформаційні системи |  |  |
| Інформаційні технології |  |  |
| Інші дисципліни (наприклад, кібернетика) |  |  |

На додаток до відмінностей у дисциплінарних підходах і типах навчальних закладів, ми визнаємо, що навчальні заклади використовують різні методи викладання (наприклад, лекції, лабораторні роботи, змішані, онлайн-заняття) і мають інші обмеження або можливості, які впливають на кількість годин, витрачених на різні теми. Хоча ми очікуємо, що будь-який навчальний план або програма навчання з кібербезпеки у широкому розумінні повинні включати в себе основні поняття з кожної галузі знань, ми також очікуємо, що включення розділів знань, глибина охоплення тем в рамках цих розділів знань і конкретні цілі навчання будуть відрізнятися. Як мінімум, ми очікуємо, що ці відмінності будуть засновані на дисциплінарному підході і типі закладу. Однак, враховуючи постійний розвиток галузі, ми очікуємо, що цим відмінностям сприятимуть і інші фактори, в тому числі розвиток нових знань.

➔ *Надайте додаткову інформацію про вашу програму, яка впливає на зміст навчального плану*.

**Інформація про навчальний заклад**

➔ *Надайте наступну інформацію*.

Назва закладу:

Розташування закладу:

Контакти факультету:

Адреса електронної пошти:

Постійна URL-адреса, де доступні додаткові матеріали та інформація (*за можливістю; це може бути посилання на перелік програм або каталогів*)

**Огляд навчального плану**

➔ *Опишіть навчальний заклад, програми і загальні вимоги до програми - вимоги до курсу, факультативи та інші вимоги*

**Таблиця розділів знань**

Кожен зразок навчального плану містить великі таблиці, які відображають курси і охоплення ними галузей знань. У цій таблиці стовпці представляють курси, а рядки - розділи знань. У наступному прикладі показано шаблон таблиці розділів знань.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Галузі знань | Розділи знань | Курс 1 | Курс 2 | Курс 3 | Курс 4 | … | Курс Х |
| Захист даних | Основні поняття | Перелік результатів навчання |  |  |  |  |  |
|  | Криптографія |  |  |  |  |  |  |
|  | Цифрова криміналістика |  |  |  |  |  |  |
|  | Цілісність даних і автентифікація |  |  |  |  |  |  |
|  | Керування доступом |  |  |  |  |  |  |
|  | Протоколи захищеного зв’язку |  |  |  |  |  |  |
|  | Криптоаналіз |  |  |  |  |  |  |
|  | Конфіденційність даних |  |  |  |  |  |  |
|  | Безпека зберігання даних |  |  |  |  |  |  |

Зразок таблиці розділів знань

➔ *Скачайте файл KnowledgeUnitTable\_Template.xls з сайту CSEC2017.org і слідуйте інструкціям, що містяться у файлі для заповнення таблиці*.

➔ *Включіть назву вашої Таблиці розділів знань до цього розділу, щоб гарантувати, що документи будуть належним чином пов’язані*.

**Аналіз навчальних планів: основні поняття та розділи знань за типовою спеціальністю**

➔ *Для типової спеціальності складіть таблицю охоплення основних понять і розділів знань. Підготуйте перелік тем, порушених у кожному курсі. Потім підготуйте загальну оцінку охоплення розділів знань. Шаблон для цієї таблиці міститься на другому листі у файлі: KnowledgeUnitTable\_Template.xls. У наступному прикладі показано шаблон таблиці охоплення розділів знань*.

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Галузі знань | Розділ знань | Курс 1 | Курс 2 | Курс 3 | Курс 4 | … | Курс Х | % охоплення | За опцією: Додаткові теми |
| Захист даних | Основні поняття | Перелік результатів навчання |  |  |  |  |  | % охоплених тем | Перелік охоплених додаткових тем |
|  | Криптографія |  |  |  |  |  |  |  |  |
|  | Цифрова криміналістика |  |  |  |  |  |  |  |  |
|  | Цілісність даних і автентифікація |  |  |  |  |  |  |  |  |
|  | Керування доступом |  |  |  |  |  |  |  |  |
|  | Протоколи захищеного зв’язку |  |  |  |  |  |  |  |  |
|  | Криптоаналіз |  |  |  |  |  |  |  |  |
|  | Конфіденційність даних |  |  |  |  |  |  |  |  |
|  | Безпека зберігання даних |  |  |  |  |  |  |  |  |

Зразок таблиці охоплення розділів знань

➔ *Надайте високорівневу картину охоплення основних понять галузей знань CSEC2017. Вкажіть відсоток основних понять для кожної галузі знань, що охоплюється навчальним планом.*

*Примітка: ця таблиця є витягом з таблиці охоплення блоків знань*.

|  |  |
| --- | --- |
| **Галузі знань** | **Охоплення основних понять** |
| *Захист даних* | % охоплення основних понять |
| *Захист програмного забезпечення* |  |
| *Захист компонентів* |  |
| *Захист з’єднань* |  |
| *Захист системи* |  |
| *Захист людини* |  |
| *Захист організації* |  |
| *Захист суспільства* |  |

**Можливі перегляди навчальних планів (на основі CSEC2017)**

➔ *Опишіть можливі зміни в навчальному плані в результаті перегляду рекомендацій щодо викладання CSEC2017*.

➔ *Опишіть всі теми навчального плану, які ви висвітлюєте і яких немає в рекомендаціях щодо викладання CSEC2017*.

**Резюме курсів**

➔ *Включіть опубліковані резюме всіх курсів, включених до вашої таблиці*.

**Зразок плану підготовки фахівців**

Сукупність знань CSEC 2017 надає гнучкість для підтримки підготовки до різних посадових ролей (або посад) в рамках галузі кібербезпеки. Приклади програм підготовки фахівців демонструють, як вимоги до посадових ролей узгоджуються з основними поняттями галузей знань і деякими підгрупами розділів знань. Наведено приклади, щоб показати різні способи, якими роботодавці можуть використовувати сукупність знань для характеристики потреб окремих посадових ролей в галузі кібербезпеки.

(Примітка: *будь ласка, видаліть виділені курсивом інструкції у ваших відповідях*.)

➔ *Надайте наступну інформацію*

ПІБ контактної особи:

Адреса електронної пошти:

Назва компанії:

Розташування (Країна): [Основне місце розташування посади.]

Посада:

**Опис посади**

➔ *Надайте опис посади і вимог до претендента (наприклад, вчений ступінь, сертифікати, досвід, знання, навички та вміння [KSA])*.

Постійна URL-адреса, де доступні додаткові матеріали та інформація (*за можливістю; це може бути посилання на сайт з останніми пропозиціями*)

**Резюме галузей знань**

➔ *Перерахуйте галузі знань і цілі навчання, які мають відношення до посади. Примітка: можливо, буде простіше заповнити цю таблицю останньою*.

|  |  |
| --- | --- |
| **Галузь знань** | **Цілі навчання** |
| *(наприклад) Захист системи* |  |
|  |  |
|  |  |

**Охоплення сукупності знань CSEC2017**

➔ *Вкажіть теми та цілі навчання (LO) для основних понять і розділів знань, необхідних для цієї посади*.

Таблиця прикладів програми підготовки фахівців знаходиться на четвертому листі файлу KnowledgeUnitTable\_Template.xls (див. таблицю нижче).

Примітка: цей розділ, ймовірно, найбільш трудомісткий, але найцінніший для педагогів, які планують прийняти рекомендації щодо викладання CSEC2017.

|  |  |  |  |
| --- | --- | --- | --- |
| Галузі знань | Розділи знань | Посада | |
| Захист даних | Основні поняття | Перелік тем | Перелік цілей навчання |
|  | Криптографія |  |  |
|  | Цифрова криміналістика |  |  |
|  | Цілісність даних і автентифікація |  |  |
|  | Керування доступом |  |  |
|  | Протоколи захищеного зв’язку |  |  |
|  | Криптоаналіз |  |  |
|  | Конфіденційність даних |  |  |
|  | Безпека зберігання даних |  |  |

Зразок таблиці розділів знань

**Додаткові теми**

➔ *Перерахуйте теми, знання, навички, вміння та/або компетенції, необхідні для цієї посади, але не включені в сукупність знань CSEC2017*.

**Інші коментарі**

➔ *Надайте будь-яку додаткову інформацію. [За опцією]*

**Зразок курсу**

Сукупність знань CSEC 2017 дозволяє гнучко підтримувати безліч різних курсів. Приклади курсів демонструють, як курси спеціалізованих закладів охоплюють основні поняття галузі знань і деякі підгрупи розділів знань. Наводяться приклади, що демонструють, яким чином сукупність знань може бути реалізована окремими курсами.

➔ *Надайте наступну інформацію*

Номер курсу, назва курсу, навчальний заклад

Розташування навчального закладу:

ПІБ контактної особи факультету:

Адреса електронної пошти:

Постійна URL-адреса, де доступні додаткові матеріали та інформація (*за можливістю; це може бути посилання на сайт курсу з останніми пропозиціями*):

**Дисциплінарний підхід і тип закладу**

➔ *Виберіть дисциплінарний підхід і тип навчального закладу, які найкраще описують вашу програму. Вкажіть основне місце розташування навчального закладу*.

|  |  |  |  |
| --- | --- | --- | --- |
|  |  | **Тип навчального закладу** | |
| **Дисциплінарний підхід** |  | Ступінь / Тривалість програми | Країна |
| Інформатика | *(наприклад) Бакалавр / 4 роки* | *(наприклад) Сполучені Штати Америки* |
| Обчислювальна техніка |  |  |
| Програмна інженерія |  |  |
| Інформаційні системи |  |  |
| Інформаційні технології |  |  |
| Інші дисципліни (наприклад, кібернетика) |  |  |

**Резюме галузей знань**

➔ *Перерахуйте галузі знань і цілі навчання, які мають відношення до курсу. Примітка: можливо, буде простіше заповнити цю таблицю останньою*.

|  |  |
| --- | --- |
| **Галузь знань** | **Цілі навчання** |
| *(наприклад) Захист системи* |  |
|  |  |
|  |  |

**Опис курсу**

➔ *Дайте відповіді на наступні питання про курс*. *Видаліть виділені курсивом інструкції у ваших відповідях*.

**Як курс вписується в вашу навчальну програму?**

*На якому курсі студенти зазвичай проходять курс? Він обов’язковий? Чи є якісь попередні умови або він викладається в послідовності курсів? В середньому, скільки студентів обирають цей курс в семестр / квартал / рік?*

**Що входить в курс?**

*Надайте короткий опис і / або короткий список тем - можливо, з вашого навчального плану. (Це, ймовірно, буде найдовша відповідь.)*

**Який формат курсу?**

*Опишіть формат курсу. Це очна форма, онлайн заняття або змішаний формат? Скільки академічних годин? Чи є лекції, лабораторні заняття або семінари?*

**Як оцінюють студентів?**

*Опишіть процес оцінювання студентів. Які типи і кількість завдань повинні виконувати студенти? (Приклади: письмові роботи, ряд задач, проекти з програмування тощо). Скільки часу, на вашу думку, студенти витрачатимуть на виконання оціночних робіт*?

**Підручники та матеріали курсу**

*Дайте короткий опис використовуваних матеріалів (наприклад, підручників, мов програмування, середовищ тощо)*

**Чому ви викладаєте цей курс таким чином?**

*Обґрунтуйте курс і цілі. Якщо ви знаєте, вкажіть історію і передісторію курсу, а також час останнього редагування / перегляду. Студенти зазвичай вважають цей курс складним?*

**Охоплення сукупності знань CSEC2017**

➔ *Вкажіть теми і цілі навчання для основних понять і розділів знань, розглянутих протягом курсу*.

Таблиця прикладів курсу знаходиться на третьому аркуші файлу KnowledgeUnitTable\_Template.xls (див. таблицю нижче).

Примітка: цей розділ, ймовірно, найбільш трудомісткий, але найцінніший для педагогів, які планують прийняти рекомендації щодо викладання CSEC2017.

|  |  |  |  |
| --- | --- | --- | --- |
| Галузі знань | Розділи знань | Курс | |
| Захист даних | Основні поняття | Перелік тем | Перелік цілей навчання |
|  | Криптографія |  |  |
|  | Цифрова криміналістика |  |  |
|  | Цілісність даних і автентифікація |  |  |
|  | Керування доступом |  |  |
|  | Протоколи захищеного зв’язку |  |  |
|  | Криптоаналіз |  |  |
|  | Конфіденційність даних |  |  |
|  | Безпека зберігання даних |  |  |

Зразок таблиці розділів знань

**Не охоплені теми розділів знань**

➔ *Для не охоплених розділів знань вкажіть, чи охоплені вони в іншому курсі або взагалі не охоплені у вашій навчальній програмі*.

**Додаткові теми**

➔ *Перерахуйте важливі теми курсу, які ви не знайдете в сукупності знань CSEC2017*.

**Інші коментарі**

➔ *Надайте додаткові коментарі [необов’язково]*

1. Див., наприклад, CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html [↑](#footnote-ref-1)
2. Див. доповідь (ISC)2 за посиланням:

   https://www.boozallen.com/content/dam/boozallen/documents/Viewpoints/2015/04/frostsullivan-ISC2-global-information-security-workforce-2015.pdf [↑](#footnote-ref-2)
3. Комітет АСМ зі складання рекомендацій щодо викладання інформатики (ACM Curriculum Committee on Computer Science). 1968 р. Навчальний план 68: Рекомендації щодо викладання інформатики в рамках навчальних програм. Ком ACM 11, 3 (березень 1968 р.), стор. 151-197. [↑](#footnote-ref-3)
4. Огляд комп’ютерних дисциплін ACM: http://acm.org/education/curricula-recommendations [↑](#footnote-ref-4)
5. Адреса веб-сайту IEEE CS: https://www.computer.org/ [↑](#footnote-ref-5)
6. Адреса веб-сайту AIS SIGSEC: http://aisnet.org/group/SIGSEC [↑](#footnote-ref-6)
7. Адреса веб-сайту IFIP WG 11.8: https://www.ifiptc11.org/wg118 [↑](#footnote-ref-7)
8. Адреса веб-сайту проекту з кібер-освіти: http://cybereducationproject.org/about/ [↑](#footnote-ref-8)
9. ISEW проводився спільно з Колоквіумом з питань освіти в галузі безпеки інформаційних систем (CISSE); спонсорами були корпорація Intel, Національний науковий фонд (NSF) та Інституту захисту інформації та інфраструктури (I3P) при Університеті Джорджа Вашингтона (GW) [↑](#footnote-ref-9)
10. Хоча ми намагалися вказати всіх учасників, якщо ми пропустили або неправильно представили вашу участь, будь ласка, зв’яжіться з нами для внесення виправлень. [↑](#footnote-ref-10)
11. Веб-сайт наукових стандартів наступного покоління Національної дослідницької ради США: http://nextgenscience.org [↑](#footnote-ref-11)
12. Національна дослідницька рада США. 2013 р. Наукові стандарти нового покоління: Для держав, від держав. Вашингтон, округ Колумбія: The National Academies Press. [↑](#footnote-ref-12)
13. Глобальне дослідження ринку фахівців з інформаційної безпеки доступно за адресою: https://iamcybersafe.org/gisws/ [↑](#footnote-ref-13)
14. Перелік професійних навичок і якостей фахівців з кібербезпеки, підготовлений Радою директорів з людського капіталу США доступний за адресою: https://www.chcoc.gov/content/competency-model-cybersecurity [↑](#footnote-ref-14)
15. Посилання: [https://www.fastcompanv.com/3034947/the-future-of-work/whv-top-tech-ceos-want-](https://www.fastcompany.com/3034947/the-future-of-work/why-top-tech-ceos-want-employees-with-liberal-arts-degrees) [employees-with-liberal-arts-degrees](https://www.fastcompany.com/3034947/the-future-of-work/why-top-tech-ceos-want-employees-with-liberal-arts-degrees) [↑](#footnote-ref-15)
16. Сайт Monster.com: [http://monster.com](http://monster.com/) [↑](#footnote-ref-16)
17. Основний план підготовки фахівців з кібербезпеки NICE: https://www.nist.gov/itl/appliedcybersecurity/national-initiative-cybersecurity-education-nice/nice-cybersecurity [↑](#footnote-ref-17)
18. Сінгапурська стратегія у галузі кібербезпеки: https://www.csa.gov.sg/news/publications/singaporecybersecurity-strategy [↑](#footnote-ref-18)
19. Національна стратегія у галузі кібербезпеки уряду Її Величності на 2016-2021 рр..:

    https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 [↑](#footnote-ref-19)
20. Категорії NCWF і відповідні вимоги можна знайти тут:

    https://www.nist.gov/itl/applied-cybersecurity/national-initiative-cybersecurity-educationnice/nice-cybersecurity [↑](#footnote-ref-20)