МІЖНАРОДНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Факультет кібербезпеки, програмної інженерії та комп'ютерних наук
Кафедра комп'ютерної інженерії та інноваційних технологій

КОНСПЕКТ ЛЕКЦІЙ

з навчальної дисципліни

«ВСТУП ДО СПЕЦІАЛЬНОСТІ»

для здобувачів вищої освіти галузі знань 12 «Інформаційні технології»
спеціальності 125 «Кібербезпека та захист інформації»
першого (бакалаврського) рівня вищої освіти

Йона Л.Г., Педяш В.В., Мазур Г.Д.

2025 рік

Затверджено Вченою Радою Міжнародного гуманітарного університету
(протокол № 5 від 20.01.2025 р.)

Йона Л.Г., Педяш В.В., Мазур Г.Д.

Вступ до спеціальності: конспект лекцій для здобувачів [Електронне видання]. / Йона Л.Г., Педяш В.В., Мазур Г.Д. Кафедра комп’ютерної інженерії та інноваційних технологій Міжнародного гуманітарного університету. Одеса, 2025. – 34 с.

Конспект лекцій з курсу «Вступ до спеціальності» розроблено відповідно до навчального плану. Матеріали призначено для студентів факультету кібербезпеки, програмної інженерії та комп’ютерних наук Міжнародного гуманітарного університету, які навчаються за першим (бакалаврським) рівнем вищої освіти в галузі знань – 12 Інформаційні технології, спеціальність 125 «Кібербезпека та захист інформації».

ЗМІСТ

ВСТУП

Сучасний світ характеризується стрімким розвитком інформаційних технологій та глобальною цифровізацією всіх сфер суспільного життя. Цей процес супроводжується значним ускладненням загроз інформаційній безпеці, появою нових видів кіберзлочинності, кібертероризму та кібершпигунства. У зв`язку з цим підготовка висококваліфікованих фахівців у галузі кібербезпеки набуває першочергового значення для забезпечення національної безпеки держави, захисту критичної інфраструктури та гарантування прав громадян у цифровому просторі.

Дисципліна «Вступ до спеціальності» є базовою для здобувачів першого (бакалаврського) рівня вищої освіти за спеціальністю 125 «Кібербезпека та захист інформації». Вона покликана сформувати у студентів системне уявлення про предмет та завдання кібербезпеки як науки і практичної діяльності, ознайомити їх із ключовими термінами, концепціями та принципами захисту інформації, а також виробити відповідальне ставлення до навчання та майбутньої професійної діяльності.

Конспект лекцій охоплює сім основних тем, логічно пов`язаних між собою та побудованих за принципом поступового ускладнення матеріалу: від загальних питань підготовки фахівців та академічної доброчесності до конкретних технічних методів захисту інформації. Особливу увагу приділено формуванню розуміння ролі здорового способу життя у забезпеченні професійної ефективності, оскільки кібербезпека є надзвичайно інтелектуально навантаженою сферою, що потребує постійного навчання та збереження когнітивного потенціалу фахівця.

Матеріал конспекту базується на чинному законодавстві України у сфері кібербезпеки та захисту інформації, міжнародних стандартах ISO/IEC 27000, NIST Cybersecurity Framework, вітчизняній та зарубіжній навчальній літературі з кібербезпеки та суміжних дисциплін.

ЛЕКЦІЯ 1

Основні складові підготовки фахівців у сфері кібербезпеки. Здоровий спосіб життя як інструмент професійної ефективності

Спеціальність 125 «Кібербезпека та захист інформації» в Україні була включена до Переліку галузей знань і спеціальностей, за якими здійснюється підготовка здобувачів вищої освіти, відповідно до постанови Кабінету Міністрів України. Вона відноситься до галузі знань 12 «Інформаційні технології» і є одним із найбільш перспективних та затребуваних напрямів підготовки у XXI столітті. Поява цієї спеціальності зумовлена зростаючою кількістю кіберінцидентів, що завдають шкоди державним органам, бізнесу та окремим громадянам, а також стратегічною необхідністю забезпечити технологічний суверенітет держави.

Кібербезпека як дисципліна знаходиться на перетині кількох наукових напрямів: комп'ютерних наук, математики, права, психології та управління. Це обумовлює широкий спектр компетентностей, якими повинен володіти випускник даної спеціальності. Серед них – глибоке розуміння принципів роботи комп'ютерних мереж і операційних систем, знання методів криптографічного захисту інформації, здатність проводити аналіз ризиків та реагувати на кіберінциденти, а також правова обізнаність у сфері захисту персональних даних і кіберзлочинності.

Підготовка фахівця з кібербезпеки охоплює три взаємопов`язані складові: фундаментальні теоретичні знання, практичні технічні навички та м'які компетентності (soft skills). Фундаментальні знання включають математику (теорію ймовірностей, математичну статистику, комбінаторику), яка є основою криптографії та аналізу вразливостей, дискретну математику та теорію алгоритмів, що необхідні для розуміння принципів роботи сучасних систем захисту, теоретичні засади мереж передачі даних та протоколів взаємодії.

Практичні технічні навички фахівця з кібербезпеки формуються у процесі роботи з реальними інструментами та системами. Це означає набуття досвіду адміністрування операційних систем сімейства Linux і Windows, роботи з мережевим обладнанням, налаштування засобів захисту інформації (міжмережевих екранів, систем виявлення вторгнень, антивірусних засобів), проведення тестування на проникнення та дослідження шкідливого програмного забезпечення. Важливим аспектом є освоєння різноманітних мов програмування – Python, C/C++, JavaScript – що дозволяє розуміти природу вразливостей на рівні коду.

М’які компетентності відіграють надзвичайно важливу роль у сфері кібербезпеки. Аналітичне мислення, здатність до системного бачення проблем, уважність до деталей, комунікативні навички (необхідні для донесення складних технічних питань до нетехнічної аудиторії) та здатність до безперервного самонавчання є обов’язковими якостями сучасного фахівця із захисту інформації. Швидкоплинність ландшафту загроз означає, що знання, отримані сьогодні, вже завтра можуть бути недостатніми, а тому вміння навчатись самостійно є однією з найцінніших якостей.

Сфера кібербезпеки відноситься до тих видів діяльності, що пов`язані з хронічним стресом, ненормованим робочим часом та великим когнітивним навантаженням. Фахівці з кібербезпеки нерідко стикаються з необхідністю вирішувати складні технічні задачі в умовах жорсткого дедлайну, реагувати на кіберінциденти в нічний час, підтримувати постійну готовність до нових загроз. Усі ці чинники роблять піклування про власне здоров’я не просто особистою справою, а професійним обов’язком.

Дослідження у галузі нейронауки переконливо свідчать про те, що регулярна фізична активність суттєво покращує когнітивні функції. Аеробні навантаження стимулюють вироблення нейротрофічного фактора мозку (BDNF), який сприяє утворенню нових нейронних зв`язків, покращує пам’ять та здатність до навчання. Для фахівця з кібербезпеки, від якого

вимагається постійне засвоєння нових знань та розв`язання нестандартних задач, це означає пряму залежність між фізичною формою та кар'єрним успіхом.

Якість сну є ще одним критично важливим чинником когнітивної ефективності. Під час сну відбуваються процеси консолідації пам'яті – перенесення інформації з короткочасної пам'яті до довгострокової. Систематичне недосипання призводить до зниження концентрації уваги, погіршення прийняття рішень та підвищення схильності до помилок – всіх тих наслідків, які є абсолютно недопустимими у сфері кібербезпеки, де одна помилка може мати катастрофічні наслідки. Рекомендований час сну для дорослої людини становить від 7 до 9 годин на добу.

Харчування безпосередньо впливає на роботу мозку. Збалансований раціон, що містить достатню кількість поліненасичених жирних кислот омега-3, вітамінів групи В, антиоксидантів та мінеральних речовин, забезпечує стабільну роботу нервової системи і знижує ризик розвитку синдрому хронічної втоми. Слід уникати надмірного вживання кофеїну як засобу підвищення продуктивності, оскільки його регулярне вживання призводить до розвитку толерантності та порушення природних ритмів сну і неспання.

Психологічне здоров'я та стресостійкість є ключовими чинниками ефективної діяльності у сфері кібербезпеки. Розвиток навичок управління стресом – медитації усвідомленості, прогресивної м`язової релаксації, технік тайм-менеджменту – дозволяє зберігати когнітивну ясність в умовах тиску. Важливим є також розвиток соціальних зв`язків та участь у професійних спільнотах, що дозволяє обмінюватись досвідом та отримувати підтримку у складних ситуаціях.

Ринок праці у сфері кібербезпеки характеризується стійким дефіцитом кваліфікованих кадрів у всьому світі. За різними оцінками, глобальна нестача фахівців з кібербезпеки становить кілька мільйонів осіб і

продовжує зростати. В Україні цей попит посилюється потребами оборонного сектору, банківської системи, телекомунікаційної галузі та органів державного управління.

Кар’єрні шляхи у кібербезпеці є надзвичайно різноманітними. Серед основних спеціалізацій виокремлюють: аналітика інформаційної безпеки, пентестера (фахівця з тестування на проникнення), інженера з безпеки хмарних систем, спеціаліста з реагування на кіберінциденти, аудитора інформаційної безпеки, архітектора систем безпеки, а також дослідника вразливостей. Кожна з цих ролей потребує специфічного набору знань і навичок, що підкреслює важливість цілеспрямованого планування власного кар’єрного шляху ще під час навчання.

ЛЕКЦІЯ 2

Академічна доброчесність: етика та відповідальність у навчанні

Академічна доброчесність є фундаментальним принципом функціонування освітнього і наукового простору, що забезпечує якість знань, довіру суспільства до наукових результатів та формує морально-етичний фундамент майбутнього фахівця. Закон України «Про освіту» (2017) визначає академічну доброчесність як сукупність етичних принципів та визначених законом правил, якими мають керуватися учасники освітнього процесу під час навчання, викладання та провадження наукової діяльності.

Ключовими принципами академічної доброчесності є: чесність – надання достовірної інформації про результати власної роботи; довіра – переконаність у достовірності наданих іншими учасниками процесу результатів; справедливість – забезпечення рівних умов оцінювання для всіх; повага – визнання авторських прав та інтелектуальної власності; відповідальність – усвідомлення наслідків власних дій у навчальній та науковій діяльності. Ці принципи взаємопов`язані і утворюють єдину систему цінностей, яка визначає поведінку доброчесного учасника академічного середовища.

Академічний плагіат є найпоширенішою формою порушення академічної доброчесності. Він полягає у навмисному або ненавмисному використанні чужих ідей, тексту, результатів досліджень або інших інтелектуальних продуктів без належного посилання на джерело та вказівки автора. Розрізняють пряме (дослівне) копіювання тексту, перефразування без вказівки на джерело, мозаїчний плагіат (поєднання фрагментів з різних джерел без посилань), самоплагіат (повторне використання власних раніше опублікованих матеріалів без відповідного позначення) та плагіат ідей (привласнення чужих концепцій без посилання).

Фабрикація та фальсифікація є серйознішими порушеннями, що полягають у вигадуванні або свідомому спотворенні результатів дослідження, даних, посилань на джерела. Ці форми порушень особливо небезпечні у сфері кібербезпеки, оскільки хибні результати досліджень у цій галузі можуть призвести до прийняття неправильних рішень щодо захисту систем і, відповідно, до реальних збитків.

Академічний обман охоплює широке коло дій: використання несанкціонованих матеріалів під час контрольних заходів, отримання або надання допомоги у виконанні оцінювальних завдань, придбання готових робіт, підробка підписів та документів. Залежно від виду та ступеня тяжкості порушення, передбачаються різноманітні наслідки: від зниження оцінки або повторного складання до відрахування з навчального закладу.

В Україні питання академічної доброчесності регулюється кількома нормативно-правовими актами. Закон України «Про освіту» встановлює загальні принципи та вимоги. Закон України «Про вищу освіту» конкретизує їх стосовно сфери вищої освіти. Важливу роль відіграє також законодавство про авторське право і суміжні права, що захищає інтелектуальну власність авторів наукових та освітніх матеріалів. Крім того, кожен заклад вищої освіти розробляє власні Положення про академічну доброчесність, що встановлюють конкретні процедури виявлення порушень та застосування відповідних заходів.

Для майбутніх фахівців з кібербезпеки академічна доброчесність має особливе значення, що виходить далеко за межі навчального процесу. По-перше, ці фахівці матимуть доступ до конфіденційної інформації, критичної для безпеки організацій, а тому питання особистої чесності та відповідальності є надзвичайно актуальними. По-друге, у сфері кібербезпеки надзвичайно важливим є дотримання авторських прав на програмне забезпечення, технічну документацію та методики тестування.

Феномен «security through obscurity» (безпека через невідомість) прямо суперечить принципам академічної доброчесності та відповідального розкриття вразливостей. Сучасна парадигма кібербезпеки базується на відкритості та обміні знаннями в межах фахової спільноти, що є неможливим без дотримання норм академічної та професійної доброчесності. Принцип відповідального розкриття (responsible disclosure) вразливостей у програмному забезпеченні є прямим відображенням цінностей академічної доброчесності у практичній площині.

Університетські знання, отримані з порушенням норм академічної доброчесності, є ненадійним фундаментом для подальшої кар'єри. Фахівець, що звик «обходити правила» у навчанні, з більшою імовірністю застосовуватиме подібні практики у професійній діяльності, що у сфері кібербезпеки може мати серйозні правові та репутаційні наслідки.

Сучасні технологічні інструменти забезпечення академічної доброчесності включають системи виявлення плагіату: Unicheck, Turnitin, Plagiarism Detector та вітчизняну систему StrikePlagiarism. Ці інструменти порівнюють текст поданої роботи з базами даних академічних публікацій, інтернет-ресурсів та раніше перевірених робіт, генеруючи звіт про відсоток збігів. Важливо розуміти, що відсоток збігів сам по собі не є показником плагіату – ключовим є аналіз характеру та контексту виявлених збігів.

Правильне цитування є практичним інструментом дотримання академічної доброчесності. Різні наукові галузі використовують різні стилі цитування: APA, MLA, Chicago, IEEE (що є найбільш поширеним у технічних дисциплінах, включаючи кібербезпеку). Оволодіння навичками коректного цитування є обов'язковою частиною академічної підготовки фахівця.

ЛЕКЦІЯ 3

Основи інформаційної безпеки: ключові поняття та визначення

Інформаційна безпека (ІБ) – це стан захищеності інформаційного середовища, що відповідає інтересам особи, суспільства та держави у сфері формування, використання і розвитку відповідного інформаційного середовища. Кібербезпека, у свою чергу, є більш вузьким поняттям і стосується захисту кіберпростору – сукупності комп'ютерних мереж, систем та технологій, що функціонують у ньому. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Інформація є центральним об'єктом захисту в інформаційній безпеці. З точки зору захисту розрізняють кілька категорій інформації: відкриту інформацію, інформацію з обмеженим доступом (конфіденційну), а також секретну інформацію, що становить державну таємницю. Кожна категорія має свій режим захисту та вимоги щодо поводження з нею. Цінність інформації для зловмисника визначається не лише її змістом, але й тим, якої шкоди може завдати її розкриття, модифікація або знищення.

Тріада ЦДД: конфіденційність, доступність, цілісність

Класична тріада інформаційної безпеки CIA (Confidentiality, Integrity, Availability) – конфіденційність, цілісність та доступність – є концептуальною основою всієї галузі. Вона визначає три ключові властивості інформації, які необхідно забезпечити для її ефективного захисту.

Конфіденційність означає захист інформації від несанкціонованого доступу, тобто гарантію того, що відомості стануть відомі лише тим суб'єктам, що мають право з ними ознайомлюватись. Порушення

конфіденційності відбувається внаслідок несанкціонованого розкриття, витоку або перехоплення інформації. Для її забезпечення застосовуються шифрування, розмежування прав доступу, фізична охорона носіїв інформації та інші засоби.

Цілісність означає захист інформації від несанкціонованої або випадкової зміни чи знищення. Вона гарантує, що отримана інформація є точно такою, якою була відправлена або збережена. Для забезпечення цілісності використовуються криптографічні хеш-функції, цифрові підписи, а також механізми контролю версій та резервного копіювання.

Доступність означає забезпечення можливості авторизованим користувачам отримати доступ до інформації або ресурсу в потрібний час. Порушення доступності відбувається внаслідок атак типу «відмова в обслуговуванні» (DoS/DDoS), технічних збоїв, стихійних лих або зловмисного знищення даних. Для її забезпечення застосовуються резервування (redundancy), системи відновлення після збоїв та балансування навантаження.

Класифікація загроз інформаційній безпеці

Загроза інформаційній безпеці – це будь-яка подія, дія або бездіяльність, що може завдати шкоди інформаційним активам. За своєю природою загрози поділяються на природні (стихійні лиха, відмови обладнання через природні процеси) та штучні, що у свою чергу поділяються на ненавмисні (помилки персоналу, апаратні збої, програмні помилки) та навмисні (цілеспрямовані кібератаки, шпигунство, диверсії).

За джерелом загрози поділяються на внутрішні (від персоналу організації або осіб, що мають фізичний або логічний доступ до систем) та зовнішні (від зловмисників, що діють поза межами організації). Важливо підкреслити, що внутрішні загрози нерідко є більш небезпечними, оскільки внутрішній порушник має більший доступ до систем і краще розуміє їхню архітектуру та слабкі місця.

За результатом реалізації виділяють загрози конфіденційності (несанкціоноване розкриття), загрози цілісності (несанкціонована модифікація або знищення) та загрози доступності (унеможливлення доступу). Важливою аналітичною категорією є вектор атаки – спосіб, за допомогою якого зловмисник отримує доступ до цільової системи. До найпоширеніших векторів атак відносяться: фішинг, використання незахищених мережевих сервісів, вразливості у програмному забезпеченні, атаки на ланцюг постачання.

Ризик у сфері інформаційної безпеки – це ймовірнісна характеристика можливих збитків від реалізації загрози. Формально ризик може бути виражений як добуток ймовірності реалізації загрози та величини потенційного збитку. Управління ризиками є ключовою функцією системи інформаційної безпеки і включає ідентифікацію активів, оцінку загроз та вразливостей, аналіз ризиків та вибір стратегії реагування.

Існують чотири основні стратегії управління ризиком: прийняття ризику (усвідомлена відмова від заходів захисту, якщо вартість захисту перевищує можливий збиток), уникнення ризику (відмова від діяльності або використання технологій, що пов`язані з неприйнятним ризиком), передача ризику (страхування, аутсорсинг окремих функцій безпеки) та зниження ризику (впровадження заходів захисту, що зменшують ймовірність реалізації загрози або потенційний збиток від неї). На практиці використовується комбінація цих стратегій залежно від характеру конкретних ризиків.

Правова база захисту інформації в Україні включає кілька рівнів. На конституційному рівні Стаття 31 гарантує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. На законодавчому рівні ключовими актами є Закони «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основні засади забезпечення кібербезпеки України», «Про захист персональних

даних» та «Про державну таємницю». На рівні підзаконних актів Кабінет Міністрів України та галузеві регулятори (ДССЗЗІ України, РНБО) видають відповідні нормативні документи та стандарти.

ЛЕКЦІЯ 4

Забезпечення надійного захисту інформації в кіберпросторі. Програма навчання працівників у сфері кібербезпеки (SAT)

Захист інформації в кіберпросторі є комплексним завданням, що потребує застосування технічних, організаційних, правових та освітніх заходів у їх взаємозв`язку. Сучасний підхід до кібербезпеки базується на моделі глибокого захисту (defense in depth), яка передбачає створення кількох незалежних рівнів захисту таким чином, що подолання одного рівня не призводить до повного компромісу системи. Цей підхід аналогічний до багатошарового захисту середньовічного замку, де зовнішній рів, кріпосний мур, внутрішній двір та донжон утворюють незалежні лінії оборони.

Архітектура Zero Trust («нульова довіра») є сучасною концептуальною основою кіберзахисту, що прийшла на зміну традиційній моделі «довіряй, але перевіряй». Її ключовий принцип – «ніколи не довіряй, завжди перевіряй» – означає відмову від концепції захищеного периметра і застосування постійної аутентифікації та авторизації для кожного запиту до ресурсів незалежно від того, надходить він зсередини чи ззовні мережі. Перехід до хмарних обчислень, мобільних пристроїв та роботи з будь-якої точки світу зробив традиційну модель периметра застарілою.

Технічні засоби захисту інформації

Міжмережеві екрани (firewall) є одним із найстаріших і водночас найбільш широко застосовуваних засобів технічного захисту. Вони контролюють мережевий трафік відповідно до заздалегідь визначених правил, дозволяючи або блокуючи передачу пакетів на основі таких параметрів, як адреси джерела і призначення, порти, протоколи та стан з’єднання. Сучасні міжмережеві екрани нового покоління (NGFW) здійснюють глибоку інспекцію пакетів (DPI) та аналіз на рівні додатків, що дозволяє виявляти загрози, замасковані у дозволеному трафіку.

Системи виявлення та запобігання вторгненням (IDS/IPS) доповнюють міжмережеві екрани, здійснюючи моніторинг мережевого трафіку та поведінки систем з метою виявлення аномалій, що свідчать про кібератаки. IDS лише повідомляє про виявлені аномалії, тоді як IPS автоматично вживає заходів для блокування шкідливого трафіку. Сучасні системи поєднують сигнатурний аналіз (порівняння з базою відомих атак) та аномалійний аналіз (виявлення відхилень від базової норми поведінки).

Системи управління інформацією та подіями безпеки (SIEM) агрегують та кореляційно аналізують події з різних джерел: мережевого обладнання, серверів, автоматизованих робочих місць, засобів захисту. Це дозволяє виявляти складні багатоетапні атаки (advanced persistent threats, APT), що у своїй сукупності становлять підозрілу картину, тоді як кожна окрема подія виглядає безневинно. Ефективна робота SIEM-системи потребує ретельної настройки правил кореляції та постійного вдосконалення.

Організаційні заходи захисту інформації

Безпекова політика є основоположним документом системи захисту інформації будь-якої організації. Вона визначає цілі і принципи забезпечення безпеки, розподіл відповідальності між посадовими особами, вимоги до захисту конкретних категорій інформаційних активів та загальний підхід до управління ризиками. Ефективна безпекова політика повинна бути реалістичною, зрозумілою всім категоріям персоналу, що підпадають під її дію, а також регулярно переглядатися і актуалізуватися.

Управління доступом є критично важливим організаційним заходом. Принцип найменших привілеїв (principle of least privilege) передбачає надання користувачам рівно тих прав доступу, що необхідні для виконання їхніх службових обов’язків, і не більше. Принцип поділу обов’язків (separation of duties) запобігає концентрації критичних повноважень в одних

руках, ускладнюючи зловживання або помилки. Ці принципи є базовими при проектуванні систем управління доступом будь-якого масштабу.

Програма навчання з питань безпеки (Security Awareness Training – SAT)

Людський чинник є найбільш вразливою ланкою в системі кібербезпеки будь-якої організації. За різними оцінками, переважна більшість успішних кібератак стає можливою внаслідок помилок або навмисних дій персоналу: відкриття фішингових листів, використання слабких паролів, несанкціоноване підключення зовнішніх пристроїв тощо. Програма навчання з питань безпеки (Security Awareness Training, SAT) спрямована на підвищення рівня обізнаності персоналу про актуальні загрози та формування безпечних практик поведінки в цифровому середовищі.

Ефективна SAT-програма будується за принципом безперервності та регулярності. Одноразові інструктажі не дозволяють сформувати стійкі навички безпечної поведінки, оскільки без регулярного підкріплення знань рівень обізнаності персоналу швидко знижується. Сучасні підходи передбачають мікронавчання (короткі регулярні модулі тривалістю 3–5 хвилин), симуляції фішингових атак для перевірки та практичного закріплення знань, гейміфікацію навчального процесу та персоналізацію контенту залежно від ролі та рівня ризику конкретного співробітника.

Ключові теми SAT-програми охоплюють: розпізнавання фішингових атак та соціальної інженерії, безпечне використання паролів та менеджерів паролів, захист робочих станцій та мобільних пристроїв, безпечна робота у мережі Інтернет та електронна пошта, фізична безпека та захист носіїв інформації, процедури реагування на підозрілі інциденти, вимоги законодавства щодо захисту персональних даних. Ефективність SAT-програми вимірюється за допомогою тестів на обізнаність, результатів симуляцій фішингових атак та відстеження поведінкових показників.

Реагування на кіберінциденти

Незважаючи на всі заходи превентивного захисту, кіберінциденти неминучі. Тому не менш важливим, ніж попередження атак, є здатність організації ефективно реагувати на них. Процес реагування на кіберінциденти включає кілька послідовних фаз: підготовку (формування команди реагування, розробку планів і процедур, підготовку інструментарію), ідентифікацію (виявлення та підтвердження факту інциденту), стримування (обмеження поширення атаки та мінімізація збитків), знешкодження (усунення причин інциденту та відновлення нормального функціонування), відновлення (повернення систем до нормального стану) та аналіз (вивчення уроків інциденту для вдосконалення системи захисту).

ЛЕКЦІЯ 5

Основні поняття та методи захисту інформації в телекомунікаційних системах

Телекомунікаційна система – це сукупність технічних засобів, протоколів та процедур, що забезпечують передачу інформації на відстань. Сучасні телекомунікаційні системи побудовані за ієрархічним принципом, де кожен рівень виконує певні функції та взаємодіє лише зі своїми сусідніми рівнями. Концептуальним фундаментом для розуміння цієї ієрархії є Еталонна модель взаємодії відкритих систем (OSI – Open Systems Interconnection), розроблена Міжнародною організацією зі стандартизації.

Модель OSI включає сім рівнів: фізичний (передача бітів через фізичне середовище), канальний (формування кадрів, адресація на рівні MAC), мережевий (маршрутизація пакетів, логічна адресація IP), транспортний (надійна передача сегментів між кінцевими точками, протоколи TCP та UDP), сеансовий (управління сеансами зв`язку), представлення (перетворення форматів даних, шифрування) та прикладний (взаємодія з прикладними програмами). Розуміння рівневої моделі є необхідним для аналізу загроз та вибору адекватних заходів захисту на кожному рівні.

Мережеві протоколи та їх вразливості

Протокол IPv4 є основою сучасного інтернету, але містить ряд вразливостей, закладених при його проектуванні, коли питання безпеки не мали пріоритету. Відсутність вбудованої аутентифікації дозволяє здійснювати підробку IP-адрес (IP spoofing), що є основою для багатьох видів атак. Протокол IPv6 усуває багато недоліків свого попередника, зокрема передбачає вбудовану підтримку IPsec, однак його масове впровадження ще не завершено.

Протокол DNS (Domain Name System) перетворює доменні імена на IP-адреси і є критично важливою інфраструктурою інтернету. Його архітектура містить кілька відомих вразливостей. DNS-спуфінг (отруєння кешу) дозволяє підмінити правильну адресу на адресу шкідливого сервера. DNS-підсилення є одним з найпотужніших методів DDoS-атак. Для захисту DNS розроблено розширення DNSSEC, що забезпечує криптографічну автентифікацію відповідей DNS-сервера, однак його впровадження відбувається повільно.

Протокол HTTP, який є основою веб-комунікацій, передає дані у відкритому вигляді, що робить його вразливим до перехоплення. Протокол HTTPS вирішує цю проблему, поєднуючи HTTP з протоколами TLS/SSL, що забезпечують шифрування, аутентифікацію сервера та (опційно) взаємну аутентифікацію. Повний перехід веб-ресурсів на HTTPS є однією з ключових тенденцій розвитку інтернет-безпеки останніх років.

Захист безпроводових мереж

Безпроводові мережі Wi-Fi є особливо вразливими з точки зору кібербезпеки, оскільки фізичне середовище передачі (радіохвилі) є загальнодоступним і не може бути обмежено у просторі так само ефективно, як кабельні з’єднання. Протокол WEP (Wired Equivalent Privacy), що використовувався для захисту ранніх мереж Wi-Fi, виявився катастрофічно ненадійним і був зламаний ще у 2001 році. Наступник WEP – протокол WPA (Wi-Fi Protected Access) – також мав суттєві недоліки.

Сучасним стандартом захисту безпроводових мереж є WPA3, що усуває більшість відомих вразливостей попередніх версій. Ключовими нововведеннями WPA3 є: використання протоколу SAE (Simultaneous Authentication of Equals) замість чотириетапного рукостискання WPA2, що усуває можливість офлайн-атак на словники; індивідуальне шифрування трафіку кожного пристрою в публічних мережах; обов’язкова підтримка кадрів управління захистом (PMF).

VPN та методи шифрування мережевого трафіку

Віртуальна приватна мережа (VPN) дозволяє створити зашифрований тунель для передачі даних через відкриті (небезпечні) мережі, імітуючи таким чином пряме приватне з'єднання. VPN широко використовується як для забезпечення безпечного віддаленого доступу співробітників до корпоративних ресурсів, так і для захисту приватності окремих користувачів в мережі Інтернет.

Протокол IPsec (Internet Protocol Security) є стандартним набором протоколів для захисту IP-комунікацій шляхом аутентифікації та шифрування кожного IP-пакета. Він може працювати у двох режимах: транспортному (шифрується лише корисне навантаження пакета) та тунельному (шифрується весь пакет, включаючи заголовки). OpenVPN є популярним відкритим рішенням для побудови VPN, що використовує протоколи SSL/TLS для шифрування. WireGuard є сучасним протоколом VPN, що відрізняється значно простішою реалізацією та більш продуктивним кодом порівняно з попередниками.

Виявлення та запобігання мережевим атакам

Атаки типу «людина посередині» (Man-in-the-Middle, MitM) є одними з найнебезпечніших загроз у телекомунікаційних системах. Зловмисник розташовується між двома легітимними учасниками обміну, перехоплюючи та потенційно модифікуючи всі повідомлення. ARP-спуфінг, DNS-спуфінг та підробка SSL-сертифікатів є найпоширенішими методами реалізації MitM-атак. Захистом від них є використання шифрування, перевірка сертифікатів, а також протоколи взаємної аутентифікації.

DDoS-атаки (Distributed Denial of Service) спрямовані на вичерпання ресурсів цільового сервера або мережі шляхом надсилання надзвичайно великого обсягу трафіку з множини скомпрометованих систем (ботнету). Захист від DDoS-атак є складним комплексним завданням, що включає використання спеціалізованих сервісів фільтрації трафіку, розподілену

архітектуру сервісів, CDN (Content Delivery Network) та механізми rate limiting.

ЛЕКЦІЯ 6

Базові поняття про криптографічний захист інформації

Криптографія – це наука про методи захисту інформації шляхом її перетворення, що унеможливлює ознайомлення з нею або її модифікацію сторонніми особами без знання спеціального секрету – ключа. Криптоаналіз – це наука, що вивчає методи подолання криптографічного захисту без знання ключа. Разом вони утворюють криптологію – фундаментальну наукову дисципліну, на якій базується більша частина сучасних технологій захисту інформації.

Основними поняттями криптографії є: відкритий текст (plaintext) – вихідне повідомлення, що підлягає захисту; шифртекст (ciphertext) – результат шифрування, нечитабельний без знання ключа; ключ – секретна інформація, що управляє процесом шифрування і розшифрування; шифр (cipher) – алгоритм перетворення відкритого тексту в шифртекст і навпаки; шифрування – процес перетворення відкритого тексту в шифртекст; розшифрування – зворотний процес.

Принцип Керкгоффса є фундаментальним принципом сучасної криптографії: безпека криптографічної системи повинна забезпечуватися виключно секретністю ключа, а не секретністю алгоритму шифрування. Алгоритм може бути загальновідомим – це навіть бажано з точки зору можливості незалежного аналізу його стійкості науковою спільнотою. Саме тому більшість сучасних криптографічних алгоритмів (AES, RSA, ECDSA) є відкритими і ретельно вивченими.

Симетрична криптографія

Симетричне шифрування є найдавнішим видом криптографії. Його відмінна риса – використання одного й того ж ключа як для шифрування, так і для розшифрування. Це забезпечує надзвичайно високу швидкість обчислень і робить симетричне шифрування незамінним для захисту

великих обсягів даних. Однак воно має принциповий недолік: необхідність безпечної передачі спільного ключа між сторонами через незахищений канал зв`язку.

Стандарт шифрування AES (Advanced Encryption Standard) є чинним федеральним стандартом США та де-факто світовим стандартом симетричного шифрування. Він замінив застарілий DES (Data Encryption Standard) та прийнятий NIST у 2001 році. AES є блочним шифром з розміром блоку 128 бітів і підтримує три довжини ключа: 128, 192 та 256 бітів. Стійкість AES до відомих атак при всіх трьох довжинах ключа є надзвичайно високою: не відомо жодної практично реалізовної атаки, що дозволяла б зламати повний AES-128 швидше, ніж повний перебір ключів.

Режими шифрування визначають, яким чином блоковий шифр застосовується для обробки даних довільної довжини. Найважливіші режими: ECB (Electronic Codebook) – найпростіший і найменш безпечний режим, де кожен блок шифрується незалежно, що дозволяє виявити повторювані патерни; CBC (Cipher Block Chaining) – кожен блок відкритого тексту перед шифруванням об’єднується (XOR) з попереднім шифртекстом; CTR (Counter) – перетворює блочний шифр на потоковий, шифруючи послідовно зростаючі лічильники; GCM (Galois/Counter Mode) – поєднує шифрування з автентифікацією, забезпечуючи одночасно конфіденційність і цілісність.

Асиметрична криптографія

Асиметричне (публічне) шифрування вирішує проблему обміну ключами шляхом використання математично пов`язаних пар ключів: публічного (відкритого) та приватного (закритого). Повідомлення, зашифроване публічним ключем, може бути розшифроване лише відповідним приватним ключем і навпаки. Публічний ключ може вільно розповсюджуватись, тоді як приватний ключ зберігається в таємниці його власником. Це усуває необхідність безпечної передачі спільного секрету.

Алгоритм RSA (Rivest-Shamir-Adleman), опублікований у 1977 році, є найстарішим і найбільш широко відомим алгоритмом асиметричного шифрування. Його безпека базується на обчислювальній складності факторизації великих цілих чисел. RSA використовується для шифрування та цифрового підпису. Для забезпечення достатнього рівня безпеки рекомендована довжина ключа RSA у наш час становить не менше 2048 бітів, а для систем з тривалим строком безпеки – 4096 бітів.

Криптографія на еліптичних кривих (Elliptic Curve Cryptography, ECC) є сучасною альтернативою RSA, що забезпечує еквівалентний рівень безпеки при значно коротших ключах. Наприклад, ключ ECC довжиною 256 бітів забезпечує приблизно такий самий рівень безпеки, що й ключ RSA довжиною 3072 біти. Це робить ECC особливо привабливою для ресурсообмежених середовищ: мобільних пристроїв, смарт-карт, пристроїв Інтернету речей. Алгоритми ECDSA (підпис) та ECDH (обмін ключами) є широко стандартизованими та підтримуються всіма сучасними криптографічними бібліотеками.

Хеш-функції та цифровий підпис

Криптографічна хеш-функція – це однобічна функція, що перетворює вхідні дані довільної довжини на хеш-значення (дайджест) фіксованої довжини. Криптографічна хеш-функція повинна задовольняти три ключові властивості: стійкість до прообразу (за заданим хешем неможливо знайти вхідні дані, що його породжують), стійкість до другого прообразу (неможливо знайти інші вхідні дані з тим самим хешем, що і заданий відкритий текст) та стійкість до колізій (неможливо знайти будь-які два різних вхідних значення з однаковим хешем).

Алгоритм SHA-256 (та більш сучасний SHA-3) є стандартом для більшості криптографічних застосувань. SHA-256 виробляє 256-бітний хеш і широко використовується в протоколах TLS, цифровому підписі, блокчейні та інших застосуваннях. Застарілі алгоритми MD5 та SHA-1 не

повинні використовуватись у нових системах, оскільки для них були знайдені практичні колізії.

Цифровий підпис забезпечує одночасно автентифікацію відправника та цілісність повідомлення. Процедура підпису: відправник обчислює хеш повідомлення і шифрує його своїм приватним ключем – результат є цифровим підписом. Перевірка: отримувач розшифровує підпис публічним ключем відправника, отримуючи хеш, і порівнює його з власноруч обчисленим хешем отриманого повідомлення. Збіг означає, що повідомлення дійсно надійшло від власника приватного ключа і не було змінено в дорозі.

Протоколи захищеного обміну ключами та PKI

Протокол Діффі-Гелмана (Diffie-Hellman, DH) вирішує задачу безпечного узгодження спільного секрету через відкритий канал. Його варіант на еліптичних кривих (ECDH) широко використовується у сучасних протоколах TLS. Властивість «ідеальної прямої секретності» (Perfect Forward Secrecy, PFS) означає, що компрометація довгострокових ключів не дозволяє розшифрувати раніше перехоплені сесії, оскільки сесійні ключі генеруються заново для кожної сесії і не зберігаються.

Інфраструктура відкритих ключів (Public Key Infrastructure, PKI) – це сукупність ролей, правил, апаратного і програмного забезпечення та процедур, що забезпечують створення, управління, розповсюдження, використання, зберігання і відкликання цифрових сертифікатів. Центральним елементом PKI є центр сертифікації (Certificate Authority, CA), що видає та підписує цифрові сертифікати, підтверджуючи відповідність публічного ключа конкретному суб’єкту.

ЛЕКЦІЯ 7

Соціальна інженерія та методи протидії її шкідливим проявам

Соціальна інженерія у контексті кібербезпеки – це сукупність психологічних маніпулятивних методів і технік, спрямованих на обман людей з метою змусити їх розкрити конфіденційну інформацію, виконати певні дії або надати несанкціонований доступ до ресурсів. На відміну від технічних атак, соціальна інженерія не потребує складних технічних знань і спрямована на вразливість людської психології, а не на вразливості програмного забезпечення.

Психологічна ефективність соціальної інженерії ґрунтується на кількох когнітивних упередженнях та соціальних нормах, що властиві більшості людей. Принцип авторитету: люди схильні виконувати вказівки тих, кого вважають авторитетом (начальники, фахівці, представники влади). Принцип терміновості та страху: відчуття тиску часу або загрози позбавляє людину здатності критично мислити. Принцип взаємності: отримавши щось від іншої людини, ми відчуваємо зобов’язання відповісти тим самим. Принцип соціального доказу: ми схильні повторювати дії, які, на нашу думку, здійснюють інші люди. Принцип симпатії: ми охочіше виконуємо прохання людей, що нам подобаються.

Класифікація атак соціальної інженерії

Фішинг є найпоширенішим видом атаки соціальної інженерії. Він полягає у розсиланні електронних листів, що імітують повідомлення від легітимних організацій (банків, державних органів, відомих сервісів) з метою змусити жертву перейти за шкідливим посиланням, відкрити інфікований вкладений файл або ввести свої облікові дані на підробленому веб-сайті. Цільовий фішинг (spear phishing) відрізняється тим, що повідомлення персоналізоване під конкретну жертву з використанням

попередньо зібраної інформації про неї, що значно підвищує ймовірність успіху атаки.

Вішинг (голосовий фішинг) – атака, що здійснюється по телефону. Зловмисник видає себе за представника банку, технічної підтримки або іншої організації та намагається отримати від жертви конфіденційну інформацію або змусити її встановити шкідливе програмне забезпечення. Смішинг – аналогічна атака через SMS-повідомлення. Квітфішинг – цілеспрямований вишинг проти конкретних осіб, зокрема керівників організацій (т.зв. «полювання на китів», whaling).

Претекстинг (pretexting) – метод, при якому зловмисник розробляє вигадану легенду (претекст) та виконує роль певного персонажа для маніпуляції жертвою. Наприклад, зловмисник може зателефонувати в організацію, представившись співробітником технічної підтримки та попросивши надати тимчасовий пароль для «перевірки системи». Бейтинг (baiting) – техніка, що використовує фізичні носії інформації: зловмисник залишає у доступних місцях USB-накопичувачі зі шкідливим програмним забезпеченням, розраховуючи на те, що цікавий або жадібний знахідник підключить їх до свого комп’ютера.

Атака «водопій» (watering hole) – стратегія, при якій зловмисник компрометує веб-сайт, що регулярно відвідується цільовою аудиторією (так само, як хижак очікує здобич біля водопою). Атаки на ланцюг постачання передбачають компрометацію постачальника програмного забезпечення або послуг для того, щоб через нього атакувати кінцеві цілі. Гучний приклад – атака SolarWinds (2020), через яку були скомпрометовані тисячі організацій у всьому світі.

Методи збору інформації для атак соціальної інженерії

Розвідка на основі відкритих джерел (OSINT – Open Source Intelligence) є ключовим підготовчим етапом для більшості атак соціальної інженерії. Зловмисники збирають інформацію про цільову організацію та її

співробітників із загальнодоступних джерел: соціальних мереж (LinkedIn, Facebook, Instagram, Twitter/X), корпоративного веб-сайту, новинних матеріалів, реєстрів юридичних осіб, технічної документації та навіть метаданих документів.

Соціальні мережі є надзвичайно цінним джерелом інформації для соціального інженера. LinkedIn надає детальну інформацію про організаційну структуру компанії, посади і повноваження конкретних співробітників, використовувані технології та бізнес-процеси. Facebook та Instagram можуть розкрити особисту інформацію про співробітників, їхні захоплення, соціальні зв`язки та навіть розклад відряджень – все це може бути використано для персоналізації атаки.

Методи протидії соціальній інженерії

Навчання та підвищення обізнаності є найефективнішим методом протидії соціальній інженерії. Співробітники, що розуміють принципи роботи соціальної інженерії та можуть розпізнати ознаки атаки, становлять суттєво меншу загрозу для організації. Програми навчання повинні охоплювати: типові сценарії фішингу та претекстингу, навички перевірки справжності запитів, процедури звітування про підозрілі контакти та поведінку. Симуляції фішингових атак є практичним інструментом перевірки готовності персоналу та визначення областей, що потребують додаткового навчання.

Технічні заходи захисту включають: впровадження систем фільтрації електронної пошти з можливістю виявлення фішингу та шкідливих вкладень; використання протоколів автентифікації електронної пошти SPF, DKIM та DMARC, що ускладнюють підробку адрес відправника; впровадження багатофакторної аутентифікації (MFA), що суттєво знижує ефективність атак, спрямованих на викрадення облікових даних; системи управління привілейованим доступом (PAM) та принцип найменших привілеїв.

Організаційні заходи включають: розробку та виконання чітких процедур верифікації особи при запитах на отримання конфіденційної інформації або виконання привілейованих дій; впровадження принципу «чотирьох очей» для критичних операцій; чіткі правила поводження з конфіденційною інформацією та класифікація інформаційних активів; процедури безпечного знищення фізичних носіїв інформації (документів, накопичувачів). Корпоративна культура, в якій заохочується повідомлення про підозрілі випадки без страху покарання за «помилкові» тривоги, є критично важливим елементом захисту.

Правові аспекти соціальної інженерії

З правової точки зору, атаки соціальної інженерії, що реалізуються у кіберпросторі, кваліфікуються переважно за статтями Кримінального кодексу України, що встановлюють відповідальність за шахрайство, несанкціоноване втручання в роботу комп'ютерних систем та мереж, незаконне отримання відомостей, що становлять державну таємницю, а також за порушення встановленого законодавством порядку захисту інформації.

Важливо підкреслити, що сам факт оволодіння методами соціальної інженерії є правомірним і необхідним для фахівців з кібербезпеки, що спеціалізуються на тестуванні на проникнення (penetration testing). Законність проведення «соціальних» тестів на проникнення визначається наявністю відповідного договору з організацією-замовником, чітким визначенням меж тестування та умов залучення персоналу. Проведення таких тестів без відповідного дозволу є незаконним і тягне кримінальну відповідальність.

СПИСОК РЕКОМЕНДОВАНОЇ ЛІТЕРАТУРИ

Нормативно-правові акти

1. Конституція України від 28 червня 1996 р. // Відомості Верховної Ради України. – 1996. – № 30. – Ст. 141.

2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII // Відомості Верховної Ради України. – 2017. – № 45. – Ст. 403.

3. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР (зі змінами) // Відомості Верховної Ради України. – 1994. – № 31. – Ст. 286.

4. Закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (зі змінами) // Відомості Верховної Ради України. – 2010. – № 34. – Ст. 481.

5. Закон України «Про вищу освіту» від 01.07.2014 № 1556-VII (зі змінами) // Відомості Верховної Ради України. – 2014. – № 37-38. – Ст. 2004.

6. Закон України «Про освіту» від 05.09.2017 № 2145-VIII // Відомості Верховної Ради України. – 2017. – № 38-39. – Ст. 380.

7. Стратегія кібербезпеки України : затверджена Указом Президента України від 26.08.2021 № 447/2021.

Підручники та навчальні посібники

8. Андрієнко В. Ю. Основи кібербезпеки : навч. посіб. / В. Ю. Андрієнко, О. Є. Архипов. – Київ : Університет «Україна», 2020. – 320 с.

9. Горбенко І. Д. Прикладна криптологія : теорія. Практика. Застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2012. – 880 с.

10. Єрмошин М. О. Захист інформаційних систем і мереж : навч. посіб. / М. О. Єрмошин, В. М. Задорожний. – Київ : НТУ «КПІ ім. Ігоря Сікорського», 2019. – 280 с.

11. Корченко О. Г. Системи захисту інформації : підручник / О. Г. Корченко. – Київ : НАУ, 2004. – 264 с.

12. Хорошко В. О. Методи та засоби захисту інформації : підручник / В. О. Хорошко, А. А. Чекатков. – Київ : Юніор, 2003. – 504 с.

13. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems / R. Anderson. – 3rd ed. – Hoboken : Wiley, 2020. – 1232 p.

14. Bishop M. Introduction to Computer Security / M. Bishop. – Boston : Addison-Wesley, 2005. – 792 p.

15. Ciampa M. Security+ Guide to Network Security Fundamentals / M. Ciampa. – 7th ed. – Boston : Cengage Learning, 2021. – 720 p.

16. Hadnagy C. Social Engineering: The Science of Human Hacking / C. Hadnagy. – 2nd ed. – Hoboken : Wiley, 2018. – 320 p.

17. Kaufman C. Network Security: Private Communication in a Public World / C. Kaufman, R. Perlman, M. Speciner. – 2nd ed. – Englewood Cliffs : Prentice Hall, 2002. – 752 p.

18. Menezes A. J. Handbook of Applied Cryptography / A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. – Boca Raton : CRC Press, 2001. – 794 p.

29. Stallings W. Cryptography and Network Security: Principles and Practice / W. Stallings. – 8th ed. – Hoboken : Pearson, 2022. – 816 p.

20. Whitman M. E. Principles of Information Security / M. E. Whitman, H. J. Mattord. – 6th ed. – Boston : Cengage Learning, 2021. – 752 p.

Стандарти та нормативні документи

21. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги. – Київ : ДП «УкрНДНЦ», 2016.

22. ДСТУ ISO/IEC 27002:2015. Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки. – Київ : ДП «УкрНДНЦ», 2016.

23. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу / ДСТСЗІ СБУ. – Київ, 1999.

24. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. – Gaithersburg : NIST, 2020.

25. NIST Cybersecurity Framework. Version 1.1. – Gaithersburg : NIST, 2018.

Інтернет-ресурси

26. Державна служба спеціального зв`язку та захисту інформації України [Електронний ресурс]. – Режим доступу: https://cip.gov.ua

27. Національний координаційний центр кібербезпеки при РНБО України [Електронний ресурс]. – Режим доступу: https://ncscc.gov.ua

28. CERT-UA. Урядова команда реагування на комп'ютерні надзвичайні події [Електронний ресурс]. – Режим доступу: https://cert.gov.ua

29. NIST Computer Security Resource Center [Electronic resource]. – Mode of access: https://csrc.nist.gov

30. OWASP Foundation [Electronic resource]. – Mode of access: https://owasp.org

31. SANS Institute: Cybersecurity Training & Certifications [Electronic resource]. – Mode of access: https://www.sans.org