РІВНЕНСЬКИЙ ДЕРЖАВНИЙ ГУМАНІТАРНИЙ УНІВЕРСИТЕТ
Факультет математики та інформатики
Кафедра цифрових технологій та методики навчання інформатики

«До захисту допущено»
Завідувач кафедри
_____ Ігор ВОЙТОВИЧ
«_____»_____2024р.
протокол №

ЧАЙКА ВОЛОДИМИР

КВАЛІФІКАЦІЙНА РОБОТА
за освітнім ступенем «магістр»
на тему:

НАВЧАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ПРОФЕСІЙНОЇ ОСВІТИ

Виконав:
здобувач ІІ курсу
групи М-ЦТ-2
спеціальності 015 «Професійна освіта (Цифрові технології)»
Володимир ЧАЙКА

Науковий керівник:
доктор педагогічних наук, професор Ігор ВОЙТОВИЧ

Рівне – 2024

АНОТАЦІЯ

ЧАЙКА Володимир. Навчання інформаційної безпеки здобувачів професійної освіти. Кваліфікаційна робота на здобуття другого (магістерського) рівня вищої освіти за спеціальністю 015 Професійна освіта (Цифрові технології). Рівненський державний гуманітарний університет – Рівне, 2024. 82 с.

Навчання інформаційної безпеки здобувачів професійної освіти є важливим аспектом підготовки фахівців, здатних ефективно протистояти сучасним загрозам у цифровому середовищі. Враховуючи, що в умовах стрімкого розвитку інформаційних технологій і глобалізації Інтернету безпека інформації стає критичним елементом будь-якої діяльності, здобувачі професійної освіти повинні бути оснащені необхідними знаннями та навичками для забезпечення захисту даних і інформаційних систем.

Основною метою навчання інформаційної безпеки є формування у студентів розуміння принципів і засобів захисту інформації, розвитку навичок роботи з сучасними засобами інформаційної безпеки, а також здатності реагувати на потенційні загрози. В умовах, коли цифрові загрози та кіберзлочинність стають дедалі серйознішою проблемою, вміння студентів розпізнавати загрози та правильно їх нейтралізувати є необхідною умовою для їхньої майбутньої професійної діяльності.

Процес навчання повинен включати як теоретичні заняття, так і практичні заняття, де студенти можуть застосовувати отримані знання на практиці. Практична частина навчання зазвичай передбачає роботу з реальними інструментами безпеки, налаштування захисту мереж і програмного забезпечення, а також участь у проведенні тестувань на проникнення для виявлення вразливостей систем.

Загальне завдання навчальних програм з інформаційної безпеки полягає в тому, щоб студенти мали чітке уявлення про принципи конфіденційності, цілісності та доступності інформації, а також знали, як ефективно протистояти атакам і мінімізувати ризики. Важливо, щоб здобувачі професійної освіти

розуміли роль інформаційної безпеки в бізнесі та організаціях, мали практичні навички з управління інформаційною безпекою і були здатні швидко реагувати на зміни в кіберсередовищі.

Крім того, особливу увагу потрібно приділяти навчанню етичних стандартів у роботі з інформацією, оскільки професіонали в галузі інформаційної безпеки часто мають доступ до конфіденційних даних і повинні дотримуватися високих етичних стандартів щодо їх зберігання та використання. Це включає не лише вміння захищати інформацію (цифрові дані) , а й розуміння юридичних аспектів, таких як захист персональних даних та дотримання відповідних законодавчих актів.

Ключові слова: інформаційна безпека, професійна освіта, здобувачі освіти, цифрові технології, захист інформації, криптографія, конфіденційність, доступність інформації

CHAYKA Volodymyr. Teaching information security to students of vocational education. Qualification work for the second (master's) level of higher education in speciality 015 Vocational Education (Digital Technologies). Rivne State University of the Humanities, Rivne, 2024. 82 p.

Teaching information security to vocational education students is an important aspect of training professionals who can effectively counter modern threats in the digital environment. Given that in the context of the rapid development of information technology and the globalisation of the Internet, information security is becoming a critical element of any activity, vocational students must be equipped with the necessary knowledge and skills to ensure the protection of data and information systems.

The main goal of information security education is to develop students' understanding of the principles and means of information protection, develop skills in working with modern information security tools, and the ability to respond to potential threats. In an environment where digital threats and cybercrime are

becoming an increasingly serious problem, students' ability to recognise threats and properly neutralise them is a prerequisite for their future professional activities.

The training process should include both theoretical classes and practical classes where students can apply the knowledge they have gained in practice. The practical part of the training usually involves working with real security tools, setting up network and software protection, and participating in penetration testing to identify system vulnerabilities.

The overall objective of information security training programmes is to ensure that students have a clear understanding of the principles of confidentiality, integrity and availability of information, and know how to effectively counter attacks and minimise risks. It is important that vocational students understand the role of information security in business and organisations, have practical skills in information security management, and are able to respond quickly to changes in the cyber environment.

In addition, special attention should be paid to training in ethical standards in handling information, as information security professionals often have access to sensitive data and must adhere to high ethical standards in its storage and use. This includes not only the ability to protect information, but also an understanding of legal aspects, such as personal data protection and compliance with relevant legislation.

Keywords: information security, vocational education, students, digital technologies, information protection, cryptography, confidentiality, information accessibility

ЗМІСТ

ВСТУП

Актуальність теми дослідження зумовлена стрімким розвитком цифрових технологій та зростаючими загрозами в кіберпросторі, які залишають під загрозу безпеку особистої та корпоративної інформації. У цьому контексті важливу роль відіграє підготовка фахівців у галузі інформаційної безпеки, здатних ефективно реагувати на ці виклики та забезпечити захист даних у різноманітних інформаційних системах. В рамках професійної освіти є основним джерелом підготовки таких фахівців, важливо повністю аналізувати існуючі методи та інструменти навчання інформаційної безпеки, які використані в освітніх закладах.

Для ефективного забезпечення інформаційної безпеки здобувачів освіти необхідно дотримуватися заходів, рекомендованих Міністерством освіти і науки України та Кіберполіцією, особливо в умовах інформаційної війни. Для забезпечення інформаційної безпеки здобувачів професійної освіти встановлено заходи правового, технічного та програмного характеру, педагогічного та організаційного, морально-етичного характеру, а також заходи щодо захисту психіки та здоров’я людини. Зазначається, що освіта та навчання здобувачів професійної освіти у сфері інформаційної безпеки має сприяти розвитку інформаційно-комунікаційних навичок, зокрема: компетентного та успішного пошуку інформації; критичне оцінювання інформації; створення, трансформація та представлення інформаційного контенту; правові принципи створення та розповсюдження інформаційного контенту; безпека та захист даних; участь в інтернет-спільнотах. В умовах глобалізації та зростання кіберзагроз особливо актуальним є питання навчання студентів професійної освіти основам інформаційної безпеки, оскільки саме від їхніх знань та навичок залежить ефективність захисту інформаційних систем і технологій на рівнях організацій та держав. Правильне формування вмінь у цій сфері дозволяє знизити ризики витоку конфіденційної інформації,

забезпечити цілість даних і підтримку стабільної роботи інформаційних технологій.

Метою цього дослідження є сучасний аналіз методів навчання інформаційної безпеки здобувачів професійної освіти, зокрема, в контексті забезпечення ефективної підготовки фахівців для боротьби з новітніми кіберзагрозами.

Завданням дослідження є:

1) вивчення існуючих підходів до навчання інформаційної безпеки,

2) аналіз програмного забезпечення та технологій, що використовуються в освітньому процесі,

3) розробка рекомендацій щодо вдосконалення навчальних курсів і програм для фахівців цієї галузі.

Об'єктом дослідження є процес навчання інформаційної безпеки здобувачів професійної освіти.

Предметом дослідження є методи і технології навчання, програмне забезпечення та інструменти, які використовуються в цьому процесі для підготовки майбутніх фахівців у сфері цифрових технологій.

Методологія дослідження включає аналіз наукових джерел, огляд сучасних навчальних програм, а також порівняльний аналіз існуючих методів і технологій навчання інформаційної безпеки. У ході дослідження використовують методи системного аналізу, синтезу та порівняння для виявлення ефективних підходів до навчання.

Сучасні здобувачі професійної освіти живуть в інформаційному суспільстві, в якому кожен медійний продукт є в певному сенсі рекламою способу життя та певних цінностей, які впливають на результати їхніх рішень. Тому в сучасних умовах необхідні фільтруючі механізми та засоби захисту від небажаних інформаційних потоків.

Апробація результатів роботи. Основні положення та результати магістерського дослідження доповідались та обговорювались на XVII Всеукраїнській науково-практичній конференції «Інформаційні технології у

професійній діяльності» (5 листопада 2024 року, м. Рівне) та на звітній конференції звітної наукової конференції викладачів, співробітників і здобувачів вищої освіти Рівненського державного гуманітарного університету 16-17 травня 2024 року.

Кваліфікаційна робота складається зі вступу, трьох розділів і висновків до кожного розділу, загальних висновків і списку використаних джерел, трьох додатків.

РОЗДІЛ 1. ПОНЯТТЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЗАКЛАДАХ ПРОФЕСІЙНОЇ ОСВІТИ

В умовах сучасних глобальних та регіональних інформаційних протистоянь, деструктивних комунікативних впливів, зіткнення національних інформаційних інтересів кількох векторів, поширення інформаційної експансії та агресії захист національного інформаційного простору та забезпечення інформаційної безпеки стає стратегічним пріоритетним завданням сучасні держави в системі глобальних інформаційних відносин. Збереження інформаційного суверенітету та формування ефективної системи безпеки в інформаційній сфері є актуальною проблемою для України, яка часто є об’єктом зовнішньої інформаційної експансії, маніпулятивних пропагандистських технологій та деструктивного інформаційного вторгнення. В умовах російсько-української війни захист національного інформаційного простору від негативних інформаційно-психологічних впливів, операцій і воєн, забезпечення інформаційної безпеки та інформаційного суверенітету набувають особливого значення і стають факторами збереження національної ідентичності України та її функціонування. як суверенна і незалежна держава.

1.1 Базові поняття інформаційної безпеки

Інформаційна безпека та проблеми захисту національного інформаційного простору досліджувалися багатьма вченими. Зокрема, проблема відображена у працях Б. Кормича, В. Ліпкана, А. Марущака, В. Петрика, В. Почепцова та інших. Проблемні питання кібербезпеки досліджували Д. Дубов, А. Бабенко, Р. Лук’янчук, В. Номоконов, В. Бурячок, В. Хавловський, М. Погорецький та інші науковці. Однак у працях зазначених спеціалістів інформаційна безпека досліджувалася як складова національної

безпеки, а не її невід’ємна частина. Поза увагою науковців залишилися проблеми чіткого розмежування інформаційних загроз, вивчення їх джерел, комплексного дослідження технологій ведення інформаційно-психологічної війни та операцій (ІПСО), а також визначення та обґрунтування методів боротьби з інформаційно-психологічними негативними впливами.

Інформаційна безпека охоплює всі аспекти захисту інформації, що зберігається, обробляється та передається в інформаційних системах. Інформаційна безпека охоплює три основні компоненти: конфіденційність, цілісність та доступність.

Конфіденційність означає захист від несанкціонованого доступу до інформації. Це важливо для забезпечення приватності даних, таких як персональні дані користувачів, комерційні та державні секрети.

Цілісність гарантує, що інформація зберігається без змін або втручання. Це важливо для запобігання випадковим або навмисним змінам даних, що можуть призвести до порушення їхньої точності.

Доступність означає, що уповноважені користувачі повинні мати можливість отримати доступ до необхідної інформації в будь-який час, коли це необхідно.

Інформаційна безпека є надзвичайно важливою не лише для компаній і державних установ, а й для всіх користувачів сучасних технологій. З розвитком цифрових технологій і глобалізацією Інтернету виникають нові загрози — від кібератак до шахрайства з використанням персональних даних. Таким чином, підготовка фахівців, здатних ефективно забезпечити безпеку даних, стала нагальною потребою для будь-якої організації чи держави.

У зв'язку з цим, навчання інформаційної безпеки в професійній освіті набуває важливості, адже саме в освітніх закладах формується базовий рівень знань і навичок, необхідних для ефективної роботи в сфері цифрових технологій. Професійні кадри повинні мати не тільки знання про основи захисту інформації, а й навички реагування на потенційні загрози, аналізу вразливостей інформаційних систем і прийняття заходів для захисту даних.

Інформаційна безпека не обмежується лише технічними аспектами, такими як програмні та апаратні засоби захисту. Вона охоплює також етичні та юридичні питання. Протягом навчання студентам важливо розуміти, що захист інформації — це не тільки технічний процес, але й правовий обов'язок. Вони повинні усвідомлювати відповідальність за обробку та зберігання персональних даних, дотримання норм захисту інтелектуальної власності та інших правових аспектів.

Системи захисту інформації вимагають також інтеграції з іншими аспектами управління організацією. Керівники, спеціалісти з інформаційної безпеки, а також співробітники організацій повинні бути освічені щодо загроз і методів захисту, розуміти принципи управління ризиками, а також розпізнавати потенційні загрози ще на етапі їх виникнення.

Особливо актуальним є питання створення навчальних програм, які включають не тільки технічні аспекти, але й етичні норми, правила безпечного використання інформаційних технологій. Тому, в рамках освітніх програм з інформаційної безпеки важливо розглядати питання конфіденційності даних, боротьби з кіберзлочинністю, а також співпраці з правоохоронними органами в разі порушень.

Крім того, знання з інформаційної безпеки повинні бути інтегровані в інші напрямки навчальних програм, наприклад, у напрямках комп'ютерних наук, програмування, розробки інформаційних систем. Водночас навчання має враховувати специфіку професійної діяльності та вимоги сучасних цифрових середовищ. Так, для фахівців, що працюють в галузі IT-безпеки, програмування або адміністрування баз даних, необхідно надавати спеціалізовані курси з глибоким вивченням шифрування даних, побудови безпечних мереж і захисту від хакерських атак.

Сучасний стан кібербезпеки вимагає від професіоналів готовності до постійного навчання, оскільки загрози в цій сфері змінюються дуже швидко. Технології, що існували кілька років тому, можуть бути вже неефективними

проти нових видів атак, тому постійне оновлення знань є обов'язковим аспектом роботи фахівця в галузі інформаційної безпеки.

Тому теоретичні основи інформаційної безпеки в професійно-технічній освіті є важливою частиною підготовки фахівців, які володіють не лише теоретичними знаннями, а й практичними навичками, необхідними для роботи в умовах швидкозмінного цифрового середовища. Успішне навчання та розвиток таких фахівців безпосередньо впливає на ефективність захисту інформаційних систем у різних організаціях та державних структурах, забезпечення надійності та безпеки даних у глобальному цифровому світі.

Розвиток науки про безпеку в напрямі інформаційної безпеки значною мірою залежить від занурення конкретного суспільства та держави в реальність інформаційного вибуху та становлення інформаційного суспільства.

Переважна більшість наукових праць з теми інформаційної безпеки починається з обґрунтування її актуальності, посилення проникнення інформаційних технологій в усі сфери життя суспільства, а також становлення інформаційного суспільства як нового етапу розвитку (типу) суспільства, в якому тема інформаційної безпеки набуває нового змісту і є предметом правового регулювання, одним із основних напрямів забезпечення національної безпеки та безпеки держав, а також передумовою забезпечення прав і свобод громадян. людини і громадянина. Отже, феномен інформаційної безпеки розглядається крізь призму практичних взаємовідносин людини з державою та суспільством, виходячи з потреб та інтересів об’єктів та суб’єктів безпеки. Безсумнівно, усвідомлена безпека може мати вирішальний вплив на зміст і розвиток соціальних процесів. Це зумовлює актуальність дослідження інформаційної безпеки як наукової категорії та як соціального явища.

Оскільки інформаційні конфлікти вважаються природним станом у конкурентній боротьбі сучасного глобалізованого світу, особлива увага приділяється питанням забезпечення інформаційної та кібернетичної безпеки

в рамках підтримки балансу інтересів на індивідуальному та суспільному рівнях, державному та міжнародно-правовому порядок [1].

Інформаційна безпека як наукова категорія трактується по-різному. Розрізняють доктринальні, енциклопедичні та нормативно-правові визначення. Суттєво відрізняються методологічні підходи, логічні прийоми їх створення та закріплення, сфери побутування та прикладного використання. Це також тому, що сама категорія безпеки неоднозначна і визначається залежно від наукової галузі, в якій вона досліджується.

Зокрема: психологи розкривають його як відчуття, сприйняття і переживання потреби захисту життєвих потреб та інтересів людини; Адвокати (юристи) – як встановлена законом система правових гарантій захисту особи і суспільства, забезпечення їх нормальної життєдіяльності, прав і свобод; Філософи - як стан, тенденції розвитку та умови життєдіяльності суспільства та його структур, що забезпечують збереження його якісної визначеності та оптимального співвідношення свободи та необхідності; Політолог - як властивість (якість) системи і результат діяльності ряду систем і органів держави, а також сам процес діяльності, спрямований на виконання поставлених завдань щодо забезпечення безпеки держави. особа, суспільство і держава [2].

Інформаційну безпеку слід розглядати з урахуванням міждисциплінарної дослідницької стратегії І. Валлерстайна, американського соціолога та історика, визнавати схожість і зв’язок між явищами і не створювати бар’єрів щодо предмета дослідження [3]. Сучасні методи дослідження базуються на різних ідеологічних позиціях щодо соціального світу та людини, по-різному вирішують дослідницькі завдання, а також використовують різні дослідницькі стратегії [3]. Корисність використання трансдисциплінарності як одного з основних методів дослідження складних багатофакторних проблем XXI століття очевидна. Про це свідчить текст «Всесвітньої декларації про вищу освіту для XXI століття: підходи та практичні дії» [4]. У статтях 5 та 6 Декларації містяться рекомендації щодо

сприяння трансдисциплінарності програм освітнього процесу та підготовки майбутніх спеціалістів до застосування трансдисциплінарних підходів до вирішення складних проблем природи та суспільства [4].

Характерною рисою наукового знання є прагнення до знання, яке ми могли б назвати істинним. Історія філософії та науки дає підстави сумніватися в можливості одностайного тлумачення такого феномену, як істина [5]. Враховуючи те, що основною проблемою філософії є співвідношення «людина– світ», процес усвідомлення людиною сутності світу свого буття і власної сутності в їх взаємозв'язку, усвідомлення внутрішнього змісту, ознак і особливостей досліджуваної концепції вважаються необхідними [6].

Як зазначається в роботах деяких вчених [7], екзистенція пов'язана з безпекою як загальним поняттям із більш широким змістом. Водночас Ліпкан В.А. стверджував, що безпека у філософському розумінні має соціальний зміст і у своїх проявах несе риси соціальності та історичності та виступає невід'ємною частиною практичної діяльності людини. Безпека поза суспільством не існує і її зміст залежить від змін, які відбуваються в організації життєдіяльності суспільства [8].

У загальносоціологічному плані категорія «безпека» характеризує певний стан людського суспільства, який забезпечує його нормальне існування та стабільний розвиток. У соціальних моделях безпека розуміється як вирішення проблеми умов для оптимального функціонування суспільства та його поступального розвитку. У широкому філософсько-світоглядному аспекті безпека є важливою проблемою як для наукового пізнання, так і для практики існування суспільства на рівні окремої держави та планети в цілому [9].

Безпека в прямому розумінні цього слова є усвідомленим явищем конкретного суб'єкта суспільних відносин. Вона виступає як прояв активності і відносної самостійності суспільної свідомості по відношенню до суспільного буття. Ось чому ідеї, почуття, знання та досвід на тему безпеки відіграють або відіграють активну, значну роль у суспільному житті. З того факту, що безпека

є усвідомленим явищем, можна зробити висновок, що усвідомлення її необхідності визначає глибоке розуміння сутності виникаючих проблем і реальних загроз. З цього випливає усвідомлення необхідності формування ефективної системи охорони та захисту як сукупності засобів, теоретичних підходів і практичних заходів, що визначають максимальну життєздатність соціальної системи з урахуванням усіх можливих загроз чи ризиків для її існування. Основою будь-якої безпеки як системи є життєво важливі інтереси особи, нації, держави чи міжнародного співтовариства.

Це проявляється як процес розуміння, сенсу і потреби усвідомленого оволодіння ідеєю безпечного існування для подальшого існування або розвитку соціальної системи.

На практичному рівні існування соціальних систем безпека не є абстрактним феноменом, відірваним від конкретних умов життя. Його зміст залежить від певних соціальних умов. Безпека – це необхідність існування людини, нації, держави, оскільки її функціонування пов’язане із задоволенням найважливішої потреби людини. Безпека пов'язана з можливістю життя, є умовою його збереження і головним критерієм ймовірного розвитку.

У сучасній науковій літературі обговорюється те, що сама постановка проблеми безпеки базується на усвідомленні загроз, тобто проблема безпеки, безпечного існування соціальної системи, пов’язується з антиподом – небезпекою чи загрозою. Такий методологічний підхід обґрунтовує, що коли небезпеки немає, потреба в безпеці, а отже, і в забезпеченні існування системи захисту, захисту, протидії та захисту усувається. Тільки наявність небезпеки визначає таку потребу. Схожої позиції дотримується Кшиштоф Лідель, польський юрист і фахівець з міжнародного тероризму. На його думку, безпека і загрози є нерозривно пов’язаними явищами. Вони є протилежними вимірниками суспільних явищ [10].

Безпека – це поняття, яке описує стан стабільності, миру та відсутності загроз. Вона носить суб'єктивний характер і є однією з основних потреб людей, соціальних груп і держав. Включає задоволення таких потреб, як існування,

виживання, цілісність, ідентичність, незалежність, мир (спокій), доступність і стабільність розвитку [12, с.27].

Історія виникнення та розвитку терміну «безпека» охоплює значний проміжок часу, який фактично збігається з появою та розвитком людства [13]. Зміна категорії безпеки відбулася разом із визначенням навколишнього середовища, пізнання природних процесів, поширення науково-технічних знань, культури тощо. Основне розуміння цієї категорії базується на утопічній ідеї, яка спонукала вчених протягом століть. - це ідея Здатності контролювати майбутнє, передбачати майбутні події та розраховувати ймовірні сценарії розвитку з максимальною ймовірністю, основною метою якої є створення ідеальних умов для розвитку людства [9]. Розуміння ідеалу включає поняття безпеки, яке визначає їх взаємодоповнюваність у системі суспільних відносин [13].

Категорія «інформаційна безпека» означає:

- законодавче оформлення державної інформаційної політики;

- створення можливостей для отримання органами державної влади, громадянами та громадськими об'єднаннями, а також іншими юридичними особами в Україні достатньої інформації для прийняття рішень відповідно до законів України;

- забезпечення свободи інформаційної діяльності та права доступу до інформації в національному інформаційному просторі України;

- комплексний розвиток інформаційної структури;

- сприяння розвитку національних інформаційних ресурсів України з урахуванням досягнень науки і техніки та особливостей духовно-культурного життя народу України;

- Створення та впровадження захищених інформаційних технологій;

- Захист майнових прав усіх учасників інформаційної діяльності в національному просторі України;

- збереження державної власності на стратегічні об'єкти інформаційної інфраструктури України;

- охорона державної таємниці, а також інформації з обмеженим доступом, яка є об'єктом права власності або є лише об'єктом володіння, користування чи розпорядження держави;

- створення загальної системи захисту інформації, зокрема захисту державної таємниці та іншої інформації з обмеженим доступом;

- Захист національного інформаційного простору України від розповсюдження інформаційної продукції, розповсюдження якої спотворено або заборонено законодавством України;

- визначення законодавством порядку доступу іноземних держав або їх представників до національних інформаційних ресурсів України та порядку використання цих ресурсів на підставі договорів з іноземними державами; – правове визначення порядку розповсюдження на території України інформаційної продукції іноземного виробництва [14, с.744].

При цьому гносеологічний зміст інформаційної безпеки зводиться, з одного боку, до небезпек і загроз, що виникають і впливають на існування об’єкта, а з іншого – до діяльнісної складової – здатності суб’єктів створити умови безпеки для існування об'єкта захисту інформації.

Логічний зміст інформаційної безпеки має особливе значення в правовому полі. Тому що нормативне закріплення як правова категорія означає, що на ньому буде побудована система захисту інформації. Через закріплення у відповідних правових нормах здійснюються регулятивна та охоронна функції права, а саме закладаються основи захисту об’єктів інформаційної безпеки та правового регулювання діяльності суб’єктів інформаційної безпеки.

Визначення логічного змісту інформаційної безпеки залежить від розвитку наукових знань, а також від розвитку механізму державного управління.

1.2 Сучасні методи навчання інформаційної безпеки в професійній освіті

Навчання інформаційної безпеки в професійних освітніх закладах є важливим етапом підготовки майбутніх фахівців у галузі цифрових технологій. Враховуючи стрімкий розвиток інформаційних технологій і збільшення кількості кіберзагроз, актуальність цієї дисципліни важко переоцінити. Університети та технічні навчальні заклади повинні забезпечити студентів не тільки теоретичними знаннями, але й практичними навичками для ефективного управління інформаційною безпекою.

Одним із основних елементів навчання є використання інтерактивних методів. Це дозволяє значно підвищити ефективність навчання, зробивши процес більш динамічним та цікавим. Студенти не лише слухають лекції та читають літературу, а й активно взаємодіють із навчальними матеріалами, тестують різні стратегії захисту, реагують на віртуальні атаки та виправляють виявлені вразливості. Зокрема, віртуальні лабораторії та симулятори стали важливими інструментами в навчанні інформаційної безпеки. Вони дозволяють створювати віртуальні середовища для тестування та розробки реалістичних сценаріїв кіберзагроз, де студенти можуть застосувати свої знання для аналізу та усунення проблем.

Використання аналогій ігор або симуляційних технологій стало популярним методом у навчанні. За допомогою ігор та симуляцій студентам надається можливість без ризику для реальних систем досліджувати різні аспекти кібербезпеки. Це включає моделювання атак, захист від зловмисного програмного забезпечення, навчання на основі реальних інцидентів з інформаційною безпекою. Подібні практичні заняття дозволяють студентам не лише засвоїти теоретичні знання, а й формувати вміння приймати рішення в умовах реальних загроз. Кожен студент може зіштовхнутися з конкретними сценаріями атак і самостійно їх нейтралізувати, що значно підвищує його практичні навички в галузі інформаційної безпеки.

Зважаючи на швидкий розвиток технологій, важливою складовою навчання є використання новітніх програмних засобів для захисту інформації, таких як антивірусні програми, фаєрволи, системи управління інформаційною безпекою (SIEM), а також інструменти для моніторингу та аналізу загроз. Оволодіння такими інструментами на практиці дозволяє студентам отримати реальні навички, які вони зможуть застосовувати в своїй майбутній професійній діяльності.

Особливе місце в сучасних методах навчання інформаційної безпеки займає перехід до комп'ютерних курсів і онлайн навчання. Використання онлайн-платформ для вивчення інформаційної безпеки дає можливість студентам навчатись у зручний для них час, за допомогою різноманітних матеріалів, таких як відеоуроки, онлайн-тести, відеоаналітика та інтерактивні курси. Такий формат навчання дозволяє підвищити рівень залученості студентів і надати їм можливість вивчати інформаційну безпеку на більш гнучкому та персоналізованому рівні. Онлайн курси та вебінари дають можливість залучати фахівців з різних регіонів і країни для надання знань з найсучасніших тем в області кібербезпеки.

Загалом, сучасні методи навчання інформаційної безпеки в професійній освіті мають бути комплексними, інтерактивними та орієнтованими на практичне застосування знань. Важливо поєднувати теоретичні аспекти з реальними кейсами, використанням новітніх технологій і програмних засобів, а також активним залученням студентів до симуляційних занять. Це дозволить підготувати висококваліфікованих фахівців, які будуть здатні ефективно протистояти сучасним кіберзагрозам і забезпечувати надійний захист інформаційних систем.

Окрім позитивних рис інформатизації освіти (посилення ролі знань, глобалізація свідомості тощо), активно досліджуються й негативні (залежність від Інтернету, послаблення соціальних зв’язків і посилення соціальної ізоляції). Соціокультурні умови та наслідки інформатизації, їхній вплив на формування особистості інформаційного суспільства є предметом

дослідження багатьох вчених: Ю. Шевченка, В. Шевченка, С.Бабаєва, А.Войскунського, Т. Воропай, П. Гнатенко, Н. Костенко, С. Оксамітна, В.Павленко, А. Ручка, Д. Швець, Р. Шульга та ін. На думку Д. Швеця [22], інформатизація освіти призводить до інформаційного перевантаження, сприяє формуванню компонентів інформаційної диспозиції, інтерналізації (засвоєння цінностей тією мірою, якою вони визначають поведінку особистості) та екстерналізації інформації. значення. Автор звертає увагу на новий тип відчуження, а саме відхід людини від реальності та занурення у віртуальний світ; Підвищення рівня агресивності через вплив агресивних комп'ютерних ігор; соціальна самоізоляція мережевого експерта, поява комп’ютерних вірусів, хакерство тощо.

Особливе місце в сучасних методах навчання інформаційної безпеки займає перехід до комп'ютерних курсів і онлайн-навчання . Використання онлайн-платформи для вивчення інформаційної безпеки дає студентам можливість навчатися в зручний для них час (Coursera , Udemy , edX), що забезпечує доступ до матеріалів, розроблених провідними університетами світу.

Наразі, єдиний з важливих складових сучасних методів навчання є практичне навчання на основі реальних кейсів. Студенти мають змогу працювати з реальними сценаріями кіберзагроз, що дозволяє їм налагоджувати навіки боротьби з атакувальними методами, такими як фішинг, DDoS-атаки, маніпуляції з даними, зловмисні програмні засоби та інші загрози. Для цього створені спеціалізовані платформи, такі як Hack The Box , TryHackMe , які пропонують симульовані кібератаки, де студенти можуть тренуватися в реальних ситуаціях без ризику для справжніх інформаційних систем.

Загалом, сучасні методи навчання інформаційної безпеки в професійній освіті мають бути комплексними, інтерактивними та орієнтованими на практичне застосування знань. Важливо поєднувати теоретичні аспекти з реальними кейсами, використанням новітніх технологій і програмних засобів,

а також активним залученням студентів до симуляційних занять. Використання сучасних онлайн-платформ, симуляторів і віртуальних лабораторій дозволяє студентам отримати реальний досвід роботи з інформаційними системами і впроваджувати свої знання в реальних умовах. Це дозволить підготувати висококваліфікованих фахівців, які будуть здатні ефективно протистояти сучасним кіберзагрозам і забезпечити надійний захист інформаційних систем.

Ще одним із аспектів сучасного навчання є використання модульного підходу . Це дозволяє студентам навчатися в більш структурованому і гнучком форматі, де кожен модуль охоплює окремий аспект інформаційної безпеки, та дає можливість вивчити конкретні теми поетапно. Такий підхід дозволяє адаптувати навчальний процес до індивідуальних потреб студентів, а також швидко регулювати зміни в технологічних вимогах і тенденціях.

Важливим напрямком є також освітні курси та сертифікації в галузі кібербезпеки CISSP (Certified Information Systems Security Professional), CEH (Certified Ethical Hacker), CompTIA Security+ , є визнаними на міжнародному рівні .

Особливої уваги потребує також навчання етичним аспектам кібербезпеки . У сучасному світі методи навчання інформаційної безпеки в професійній освіті повинні включати інтерактивні підходи, використання нових технологій, гнучкі модульні курси, сертифікацію та етичні аспекти. Це дозволяє не тільки підготувати студентів до швидко зміненого світу кібербезпеки, а й сформувати їхні особистісні стійкі якості.

1.3 Інформаційна безпека в умовах закладу професійної освіти

Забезпечення інформаційної безпеки є важливою складовою частиною захисту інформаційних систем від несанкціонованого доступу, змін, втрати або пошкодження даних. Сучасні програмні засоби для забезпечення інформаційної безпеки дозволяють ефективно виявляти, запобігати та

нейтралізувати загрози, а також забезпечують безпеку на різних етапах обробки та зберігання даних. Ось основні категорії програмних засобів, які використовуються для забезпечення інформаційної безпеки:

1. Антивірусні програми

Антивірусні програми є основним інструментом для боротьби з вірусами та іншими шкідливими програмами, такими як трояни, черв'яки тощо. Вони працюють на основі різних технологій, включаючи визначення сигнатур вірусів, поведінковий аналіз, а також методи емулювання для виявлення нових та невідомих загроз.

- **Kaspersky Anti-Virus**: один із лідерів серед антивірусних програм, який забезпечує захист від різних типів шкідливих програм, а також надає додаткові функції для захисту від фішингу та спроб несанкціонованого доступу.
- **McAfee**: популярна програма для комплексного захисту від вірусів, що включає не тільки антивірус, а й фаєрволи, інструменти для безпеки в Інтернеті, захист від крадіжки особистих даних.
- **Bitdefender**: програма, що використовує кілька рівнів захисту, включаючи аналіз поведінки програм та перевірку на основі машинного навчання для виявлення нових загроз.

Антивірусні програми допомагають захистити системи від шкідливих програм і забезпечують базовий рівень інформаційної безпеки.

2. Фаєрволи (Firewall)

Фаєрволи — це програмні або апаратні засоби, що контролюють трафік між комп'ютерними мережами, дозволяючи або блокуючи певні типи трафіку в залежності від налаштувань безпеки. Вони застосовуються для запобігання несанкціонованому доступу до або з комп'ютерних мереж.

- **ZoneAlarm**: популярний фаєрвол для захисту від несанкціонованого доступу з Інтернету, який дозволяє блокувати вхідні та вихідні з'єднання.

- **Comodo Firewall**: надає потужні можливості для моніторингу і контролю трафіку в реальному часі, а також включає функцію «sandboxing» для безпечного тестування нових програм.
- **pfSense**: open-source фаєрвол і маршрутизатор на основі FreeBSD, який пропонує розширені функції для мережевого моніторингу, VPN, а також систему управління вхідним і вихідним трафіком.

Фаєрволи є критичними для забезпечення безпеки мереж і систем від можливих атак і несанкціонованого доступу.

3. Системи виявлення та запобігання вторгненням (IDS/IPS)

Системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS) використовуються для моніторингу та аналізу мережевого трафіку з метою виявлення та запобігання несанкціонованому доступу або іншим шкідливим діям.

- **Snort**: система виявлення вторгнень з відкритим кодом, яка дозволяє виявляти та блокувати атаки в режимі реального часу.
- **Suricata**: система для виявлення та запобігання вторгненням, яка підтримує високопродуктивне моніторинг і аналіз трафіку, включаючи аналіз по протоколах TCP/IP, HTTP, DNS і інших.
- **Bro (Zeek)**: розширена система моніторингу мережевого трафіку, що використовує скрипти для виявлення загроз і атак.

IDS/IPS є важливими інструментами для забезпечення активного захисту від атак та їх автоматичного блокування.

4. Системи управління інформаційною безпекою (SIEM)

Системи управління інформаційною безпекою (SIEM) є важливими інструментами для збору, аналізу та кореляції даних з різних джерел в межах організації. Вони дозволяють забезпечити моніторинг інформаційних систем у реальному часі та виявляти потенційні загрози або порушення політик безпеки.

- **Splunk**: одна з провідних систем SIEM, яка дозволяє збирати і аналізувати дані з різних джерел для виявлення загроз і керування інцидентами безпеки.
- **IBM QRadar**: потужна платформа для виявлення загроз і управління інцидентами, що автоматизує моніторинг безпеки та аналіз даних в реальному часі.
- **ArcSight**: система для кореляції та моніторингу безпеки, що дозволяє автоматизувати виявлення аномальних подій і швидко реагувати на інциденти.

SIEM системи допомагають здійснювати централізований моніторинг, що дозволяє своєчасно виявляти загрози та здійснювати відповідні заходи для їх усунення.

5. Криптографічні інструменти

Шифрування даних є одним з основних методів захисту інформації від несанкціонованого доступу. Програмні засоби для шифрування дозволяють забезпечити конфіденційність даних при їх зберіганні або передачі.

- **VeraCrypt**: потужний інструмент для створення зашифрованих томів і шифрування дисків. Це програмне забезпечення є безкоштовним та підтримує сучасні алгоритми шифрування.
- **GPG (GNU Privacy Guard)**: відкритий інструмент для шифрування та підпису даних, що використовується для забезпечення конфіденційності при обміні електронними листами або файлами.
- **OpenSSL**: інструмент для реалізації шифрування даних за допомогою стандартів SSL і TLS, широко використовується для забезпечення безпечних з'єднань в Інтернеті.

Криптографія є важливим елементом для захисту даних, особливо в умовах швидкого розвитку технологій і збільшення ризиків крадіжки або витоку даних.

6. Інструменти для тестування на проникнення (Pentesting)

Тестування на проникнення є важливим методом для оцінки безпеки інформаційної системи шляхом імітації реальних атак. Інструменти для тестування на проникнення допомагають фахівцям виявляти вразливості в системах до того, як ними можуть скористатися зловмисники.

- **Kali Linux**: спеціалізована операційна система, що містить набір інструментів для тестування на проникнення, аналізу вразливостей і вивчення кіберзагроз.
- **Metasploit**: платформа для тестування на проникнення, яка дозволяє автоматизувати процес виявлення вразливостей та їх експлуатації.
- **Nessus**: програма для сканування вразливостей, яка дозволяє виявляти слабкі місця в мережевих системах і додатках.

Інструменти для тестування на проникнення дозволяють фахівцям виявляти вразливості на ранніх етапах і усувати їх до того, як вони будуть використані хакерами.

7. Інструменти для аналізу мережевих загроз

Програмні засоби для моніторингу мережевого трафіку дозволяють відслідковувати та аналізувати дані, що проходять через мережу, для виявлення підозрілих або несанкціонованих дій.

- **Wireshark**: найпопулярніший інструмент для аналізу мережевого трафіку. Використовується для зняття пакетів, їх аналізу та пошуку

аномалій.

- **Tcpdump**: командний інструмент для захоплення мережевого трафіку, що дозволяє швидко отримати інформацію про з'єднання та їх зміст.

Ці інструменти допомагають моніторити трафік та швидко реагувати на мережеві загрози.

Програмні засоби для забезпечення інформаційної безпеки є важливими інструментами для захисту інформаційних систем і даних. Використання таких засобів дозволяє фахівцям ефективно виявляти та нейтралізувати загрози, забезпечувати конфіденційність та цілісність даних, а також

контролювати доступ до ресурсів. Вони є основою для забезпечення безпеки в умовах постійно зростаючих ризиків у цифровому середовищі.

На основі аналізу [24] виділимо такі типи загроз:

«1) Загрози особистій безпеці

- ризик контакту з матеріалами небажаного змісту (порнографія, нецензурна лексика, суїцидальні думки, сектантство, расизм і ненависть, вибухові речовини, хакерські сайти)

- ризик отримання недостовірної інформації

- можливі залежності (комп'ютер, ігри, Інтернет тощо)

- небезпека спілкування з небезпечними людьми (шахраї, збоченці, шахраї та ін.)

- Погрози незаконними діями (злом, порушення авторських прав тощо)

2) Загрози розголошення особистої інформації

- Погроза розголошення конфіденційних даних (ім'я, ім'я, адреса, номери кредитних карток, телефон тощо).

3) Загрози для персональних комп'ютерів

- небезпека зараження вірусами

- ризик завантаження шкідливого активного коду

- загроза завантаження програм із прихованими функціями: троянів, клавіатурних шпигунів тощо».

1.4 Основні методи попередження доступу здобувачів професійної освіти до небажаного змісту

Проблему доступу здобувачів освіти до небажаного контенту можна вирішити не одним методом, а комплексом програмних, педагогічних та організаційних заходів. Розглянемо основні з них:

Контент-фільтр – це система, яка блокує доступ до небажаних інтернет-ресурсів за певними критеріями. Контент-фільтри можуть бути реалізовані в різних програмних пакетах або як окремий програмний продукт. Наприклад, у

складі мережевих екранів або проксі-серверів. Мережеві брандмауери призначені для обмеження доступу між різними мережами, перевірки всього трафіку, що проходить через них, і блокування забороненого трафіку.

Вибрані веб-сайти – діапазон веб-сайтів, до яких діти мають доступ, визначається заздалегідь. Найчастіше використовується, коли NCC не може отримати прямий доступ до Інтернету.

Дитячі пошукові системи - це ті, які створені спеціально для дітей шкільного віку на основі існуючих пошукових систем і фільтрують видаються користувачеві посилання за віковими обмеженнями. На базі Google вчителі можуть створювати власні тематичні пошукові системи, щоб здобувачі професійної освіти не «перелопатили» весь Інтернет у пошуках потрібної інформації. Усі користувачі, зареєстровані в офісі Google, разом редагують і вдосконалюють ці пошукові системи.

Таким чином можна вирішити проблему захисту здобувачів освіти від нерелевантної інформації, яку вони можуть отримати за допомогою пошуку в пошукових системах «загального використання».

Інші методи захисту неповнолітніх користувачів:

- Моніторинг використання чату. Використання чату в освітніх цілях завжди має відбуватися під наглядом викладача;

- спеціально розроблена система електронної пошти. Це шкільний поштовий сервер із налаштованими обмеженнями щодо того, кому та як можна надсилати електронні листи. Заклади професійної освіти можуть обмежити спілкування електронною поштою лише для внутрішніх користувачів і дозволити зовнішнє спілкування лише через викладачів. Деяким здобувачам професійної освіти може бути дозволено надсилати електронні листи на зовнішні адреси, але лише за попередньо визначеним списком.

- Використання систем моніторингу. Для моніторингу найкраще використовувати програми, які дозволяють спостерігати за діями здобувачів

освіти з комп’ютера вчителя. Обов’язковим є ведення журналів їхньої активності в Інтернеті.

Досі ми говорили про те, що у навчального закладу є проблема з проникненням небажаного контенту в освітню мережу. Але є також проблема витоку контенту. У цьому випадку мова в першу чергу йде про передачу приватних персональних даних. У сучасному суспільстві існує проблема викрадення дітей, сексуальних домагань тощо. Тому особиста інформація про дитину (фото, розклад занять, електронна пошта, номер телефону) не повинна розміщуватися в Інтернеті у вільному доступі.

Публікуючи фотографії в Інтернеті (наприклад, на шкільному веб-сайті), бажано публікувати фотографії дітей лише за згодою батьків або лише групою. Імена дітей та іншу особисту інформацію (цифрові дані) надавати не можна.

Друга проблема – розсилка поштою або розміщення забороненого контенту на шкільному (або іншому) сайті. Розсилання піратських копій, порнографії тощо.

Небажаний контент потрапляє в мережу навчального закладу переважно через два канали: веб-трафік та трафік електронної пошти.

Проблему фільтрації трафіку електронної пошти зазвичай називають проблемою спаму. Образливі повідомлення, заклики до насильства тощо можуть поширюватися як спам. На додаток до всіх проблем, перерахованих вище, спам також створює надмірний трафік і відволікає користувачів.

Звичайно, важливо запобігти розповсюдженню та видаленню такого вмісту з флеш-накопичувачів NCC, CD, DVD та жорстких дисків.

Трафікомісткі процедури - завантаження відео, музики, архівів файлів програмного забезпечення - призводять до різкого збільшення трафіку даних, що може уповільнити роботу мережі та збільшити витрати на оплату трафіку даних. Більшість програм, які блокують доступ до заборонених сайтів, також дозволяють контролювати операції з інтенсивним трафіком.

Перш за все, слід зазначити, що проблема захисту від шкідливого контенту – це не лише шкільна проблема. Використання Інтернету працівниками або здобувачами професійної освіти, не пов’язане з навчальною чи службовою діяльністю, називається «кіберслакінгом» (від англ. cyberslacking).

Навчальні заклади були далеко не першими, хто спробував вирішити проблему інтернет-фільтрації. Це говорить, з одного боку, про те, що проблема глобальна і її просто неможливо вирішити, а з іншого боку, що в деяких випадках рішення, створені для організацій широкого профілю, можуть підійти для навчальних закладів. Слід також зазначити, що віруси, трояни, шпигунське програмне забезпечення та інший шкідливий код також можна легко передавати через Інтернет.

Боротьбу можна поділити на організаційні (призначення відповідальних, створення пропускного режиму для комп’ютерних класів, навчання здобувачів освіти нормам поведінки в Інтернеті, відповідальність за протиправні дії тощо) та технічні заходи. Технічні заходи включають фільтрацію трафіку та моніторинг дій тих, хто бажає отримати професійне навчання.

Моніторинг (навіть без фільтрації) вже може бути ефективним заходом. Якщо учень знає, що він робить (усі відвідування постійно контролюються і всі його дії фіксуються в лог-файлах, де вказано, хто, коли і що відвідував), ймовірність відвідування небажаних сайтів значно знижується. Давайте розглянемо параметри фільтра. Вміст можна фільтрувати на рівні провайдера, на рівні шлюзу до мережі Інтернет, яку потрібно захистити, і на рівні клієнтської станції.

Фільтрація може бути побудована на основі зовнішньої оновлюваної бази заборонених ресурсів, а може бути побудована на базі локальної програми, що працює за власними принципами фільтрації («чорні», «білі» списки, ключові слова тощо).

В основному фільтрацію можна побудувати за принципом: 1. «Ми забороняємо все, крім можливого» 2. «Можливо все, крім того, що заборонено». Звичайно, фільтрацію можна реалізувати за принципом «Ми забороняємо» все крім того, що можливо» побудувати досить легко, така форма може мати сенс для молодших школярів, але в цьому випадку Інтернет втрачає багато своїх функцій.

Другий варіант вимагає побудови та постійного оновлення величезної бази (вона повинна підтримуватися постачальником послуг), яка постійно поповнює базу забороненим контентом.

Для повноцінної реалізації другого типу фільтрації необхідно проіндексувати мільярди веб-сторінок, що під силу, наприклад, лише великим провайдерам такого сервісу, як iSS, Proventia Web Filter. Чим більше основа, тим краще і дорожче рішення.

Щодня в Інтернеті з’являються тисячі нових веб-сайтів. Тому навіть при відновленні баз з небажаними ресурсами неможливо досягти 100% фільтрації. Ще однією проблемою є неналежне фільтрування російського та україномовного контенту західними продуктами. Можливі помилки, коли фільтр відфільтровує веб-сайти з корисним вмістом. Загалом, чим розумніший фільтр і чим більша база даних, на якій він базується, тим дорожче рішення та менш доступне для шкіл.

У закладах освіти часто встановлені різні комп’ютерні пристрої та програмні продукти для фільтрації контенту (веб та електронна пошта), які працюють на різних платформах. Адміністратори професійного навчального закладу мають різний рівень досвіду роботи з комп’ютерами, і навіть неспеціаліст повинен мати змогу створювати політику фільтрації та керувати нею. Навчальний процес охоплює багато різних галузей науки, і фільтрація має бути комплексною, настроюваною, а також забезпечувати захист від новітніх загроз.

Навчання інформаційної безпеки в професійній освіті стикається з низкою проблем та викликів, які можуть ускладнити процес підготовки

фахівців у цій галузі. Зокрема, швидкий розвиток кіберзагроз, відсутність оновлених навчальних програм, а також інтеграція нових технологій у навчальний процес — це лише кілька з багатьох факторів, які можуть впливати на ефективність навчання.

Однією з основних проблем є **недоліки в навчальних програмах**, які часто не відповідають вимогам сучасного кіберпростору. Навчальні плани в ряді випадків застаріли або не охоплюють актуальні загрози, з якими стикаються професіонали у сфері інформаційної безпеки. Багато програм зосереджуються на теоретичних аспектах і не надають достатньо можливостей для здобуття практичних навичок.

Це означає, що студенти можуть завершити навчання без реального досвіду роботи з сучасними інструментами та технологіями, такими як системи управління інформаційною безпекою (SIEM), інструменти для тестування на проникнення чи аналізу мережевих загроз. Крім того, з огляду на стрімкий розвиток кіберзагроз, навчальні курси не завжди встигають включити новітні методи захисту та виявлення атак.

Кіберзагрози змінюються настільки швидко, що навчальні програми часто не встигають за ними. Це створює величезні труднощі для освіти в галузі інформаційної безпеки, оскільки студентам необхідно постійно оновлювати свої знання і навички, щоб бути готовими до нових викликів. Технології хакерських атак і методи їх обходу постійно еволюціонують, тому навчання повинно бути максимально адаптивним до нових тенденцій.

Крім того, студенти повинні бути готові до роботи з новими типами атак, такими як **атаки на об'єкти інтернету речей (IoT)**, **загрози для хмарних середовищ** або **мобільних платформ**, що вимагає гнучкості від освітніх програм у постійному оновленні матеріалів і технологій.

Інтеграція новітніх технологій в навчальний процес є важливим аспектом підготовки фахівців з інформаційної безпеки. Однак цей процес стикається з рядом проблем. Однією з основних є **відсутність ресурсів**, зокрема фінансування для закупівлі ліцензійного програмного забезпечення та

оновлення інфраструктури для використання новітніх технологій. Багато навчальних закладів не мають доступу до актуальних інструментів і програм, які є важливими для практичного навчання.

Також слід врахувати, що впровадження нових технологій у навчальний процес вимагає підготовки викладачів. Вони повинні володіти знаннями не тільки з теоретичних аспектів безпеки, але й практичними навичками роботи з новими інструментами та технологіями. Це потребує постійного професійного розвитку та навчання викладачів.

Інформаційна безпека сьогодні вимагає міждисциплінарного підходу, адже виклики, з якими стикаються фахівці, стосуються не лише технічних аспектів, але й юридичних, етичних, організаційних питань. Студенти повинні не лише знати, як захистити інформацію, але й розуміти юридичні аспекти її обробки та зберігання, а також вплив кібербезпеки на бізнес-процеси та національну безпеку.

Тому важливим завданням є інтеграція курсу з інформаційної безпеки з іншими дисциплінами, такими як право, економіка, управління бізнесом, для створення комплексної картини безпеки в організації та державі. Це дозволить підготувати спеціалістів, які будуть здатні не лише реагувати на технічні загрози, але й оцінювати їх наслідки для бізнесу та національної безпеки.

Кіберзагрози швидко змінюються, і це вимагає постійного адаптування освітніх програм до нових реалій. Студенти мають бути готові не лише до роботи з уже відомими інструментами та методами захисту, а й до швидкого освоєння нових технологій. Це вимагає від навчальних закладів постійного оновлення навчальних планів та методик, що може бути викликом для деяких освітніх установ, які не мають можливості швидко реагувати на зміни у технологічному середовищі.

Ще однією проблемою є різний рівень підготовки студентів, які вступають на спеціальності в галузі інформаційної безпеки. Деякі студенти вже мають базові знання з комп'ютерних наук, тоді як інші тільки починають знайомство з цією дисципліною. Це створює труднощі у викладанні, адже

важливо забезпечити доступність матеріалу для студентів з різним рівнем підготовки, але водночас не втратити глибину і складність теми.

Проблеми, з якими стикається навчання інформаційної безпеки, вимагають системного підходу до вдосконалення навчальних програм, адаптації до нових технологій та постійного оновлення знань і навичок студентів. Це дозволить не тільки підготувати студентів до реальних кіберзагроз, але й забезпечити їх готовність до ефективної роботи в умовах швидко змінюваного технологічного середовища.

Висновки до розділу 1

1) Інформаційна безпека є невід’ємною частиною функціонування будь-якої освітньої установи, зокрема закладів професійної освіти. Це не лише захист інформаційних ресурсів і даних від несанкціонованого доступу, але й забезпечення конфіденційності, цілісності та доступності інформації в процесі навчання. У рамках цього поняття, інформаційна безпека охоплює всі етапи обробки та зберігання даних — від їх створення до використання в освітньому процесі.

2) Зі збільшенням використання цифрових технологій у навчальних закладах, зокрема через онлайн-освіту та електронні ресурси, значно зростають ризики, пов’язані з порушенням інформаційної безпеки. Це включає кіберзагрози, такі як хакерські атаки, фішинг, витік персональних даних, а також несанкціонований доступ до академічних та фінансових даних. У зв'язку з цим важливо здійснювати комплексний захист від можливих загроз і забезпечити безпечну роботу інформаційних систем.

3) Поняття інформаційної безпеки в закладах професійної освіти має бути інтегровано в усі аспекти навчального процесу, починаючи з навчальних програм і закінчуючи внутрішніми політиками безпеки. Студенти повинні не лише засвоювати технічні знання про захист інформаційних систем, але й усвідомлювати етичні та правові аспекти захисту даних. Формування відповідального ставлення до інформаційної безпеки в студентів є важливим етапом у підготовці фахівців.

4) У навчальних закладах професійної освіти необхідно застосовувати практичні методи для забезпечення інформаційної безпеки. Це включає навчання студентів технічним навичкам, таким як налаштування безпеки в комп’ютерних мережах, управління доступом до даних, використання криптографічних методів захисту та забезпечення безпеки хмарних сервісів. Важливо також організувати тренування і симуляції для студентів, де вони можуть на практиці працювати з реальними інструментами і реагувати на кіберзагрози.

5) Заклади професійної освіти повинні також звертати увагу на правові аспекти інформаційної безпеки. Законодавство щодо захисту персональних даних та кіберзагроз постійно змінюється, і важливо, щоб студенти мали уявлення про вимоги законодавства у цій сфері. Відповідальність за порушення цих норм може мати серйозні наслідки, тому важливо, щоб студенти мали чітке розуміння етичних та юридичних норм при обробці та зберіганні інформації.

6) Забезпечення ефективної інформаційної безпеки в навчальних закладах неможливе без належної технічної інфраструктури. Це включає сучасні засоби захисту інформації, як-от фаєрволи, системи моніторингу та управління безпекою, програмне забезпечення для захисту від вірусів і шкідливих програм, а також засоби для шифрування даних. Технічна інфраструктура повинна бути постійно оновлювана та вдосконалювана для відповідності новим вимогам кібербезпеки.

7) Конфіденційність, цілісність та доступність інформації є основними принципами інформаційної безпеки. Забезпечення цих принципів є критично важливим для закладів професійної освіти, де зберігаються особисті дані студентів, академічні досягнення та інші конфіденційні матеріали. Тому важливо впроваджувати ефективні заходи для захисту цих даних, включаючи використання шифрування, системи управління доступом та аудиту.

8) Інформаційна безпека в закладах професійної освіти вимагає постійного вдосконалення політик і стратегій. Кіберзагрози постійно змінюються, тому для забезпечення безпеки необхідно регулярно переглядати політики безпеки, проводити аудит і оцінку ризиків, впроваджувати нові технології для боротьби з кіберзагрозами. Це допоможе навчальним закладам залишатися на крок попереду в умовах швидкої еволюції загроз.

РОЗДІЛ 2. МЕТОДИ ТА ЗАСОБИ НАВЧАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗДОБУВАЧІВ ЗАКЛАДІВ ПРОФЕСІЙНОЇ ОСВІТИ

Технічні або програмні засоби, окремо розглянуті, не можуть функціонувати без організованої та цілеспрямованої діяльності всіх учасників інформаційних взаємодій, без регламентації, розробки та реалізації правил інформаційної безпеки (політики безпеки), постійного керівництва обслуговуючим персоналом та управління системою інформаційної безпеки навчальних комп'ютерних центрів (СІБ НКЦ). «Усі зусилля із забезпечення внутрішньої безпеки комп'ютерних систем зосереджені на створенні надійних і зручних механізмів регулювання дій усіх легітимних користувачів і співробітників сервісу та їх обов'язку беззастережно дотримуватись регламенту доступу до ресурсів системи, встановленого в освітньому закладі. установа. Потрібні організаційні заходи для забезпечення ефективної реалізації інших захисних заходів у сфері регулювання дій людей» [25, с.31]. Оскільки на даному етапі інформатизації загальноосвітніх навчальних закладів виникають труднощі з отриманням коштів на закупівлю або оновлення. Для забезпечення обладнання та програмного забезпечення ми можемо використовувати лише наявні можливості для захисту NCC. Тому найбільш перспективним є максимальне використання організаційно-педагогічних заходів для підвищення ефективності СІБ НКЦ, реалізація яких не потребує витрат додаткових коштів. Саме комплексний підхід до інформаційної безпеки НКЦ, усвідомлення необхідності таких заходів на всіх рівнях управління освітою, навчання та підвищення кваліфікації обслуговуючого персоналу та викладачів ІТ є запорукою успішної реалізації вимог до надійність програмної складової НКЦ.

2.1 Сучасні методи навчання інформаційної безпеки

Сучасні методи навчання інформаційної безпеки повинні бути адаптовані до швидко зміненого світу технологій і загроз. Враховуючи, що кіберзагрози залишаються більш складними та різноманітними, традиційні підходи до навчання вимагають модернізації. Найефективнішими є інтерактивні методи, які поєднують теоретичні знання з практичними навичками. Інтерактивні методи навчання стають основними в сучасному навчальному процесі. Вони включають у себе використання активних форм навчання, де студент активно взаємодіє з навчальним матеріалом, а не просто сприймає його. Це дозволяє значно підвищити рівень усвідомлення і запам'ятовування інформації, оскільки студент лише не отримує знань, а й застосовує їх на практиці.

До інтерактивних методів навчання відносяться:

- **Обговорення кейсів** : Студенти аналізують реальні інциденти з інформаційної безпеки, обговорюють їх слідки та розробляють стратегії запобігання подібним ситуаціям у майбутньому.
- **Рольові ігри** : Студенти можуть виконувати роль, наприклад, фахівця з кібербезпеки або хакера, який дає змогу отримати обидві сторони протидії загрозам.
- **Групова робота та проекти** : Студенти працюють у командах, що дозволяють не лише глибше зрозуміти проблеми безпеки, а й розвивати комунікаційні навички, необхідні для ефективної роботи у сфері кібербезпеки.

Одним із важливих інструментів для навчання є **віртуальні лабораторії** . Вони не зможуть студентам працювати з реальними інструментами безпеки, тестувати інформаційні системи на вразливості та реагувати на якісь загрози в контрольованому середовищі. Це дозволяє уникнути ризику порушення реальної системи під час навчання, одночасно даючи студентам можливість отримати практичний навичок.

Наприклад, віртуальні лабораторії можуть включати:

- **Симуляції атак** : Студенти можуть виступати як захисники або зловмисники, що дає їм можливість навчитися, як захищатися від атак, так і розуміти методи їх проведення.
- **Практика з реальними інструментами** : Віртуальні лабораторії надають доступ до інструментів для тестування на проникнення, сканування вразливостей, роботи з системами SIEM та іншими програмними засобами.

Серед платформ, які широко застосовуються для таких навчальних симуляцій, можна зазначити **TryHackMe** та **Hack The Box** , де студенти проходять практичні курси, які імітують реальну ситуацію в кібербезпеці.

Модульний підхід до навчання дозволяє організувати курси, де кожен модуль охоплює окрему тему або аспект інформаційної безпеки, наприклад, криптографія, захист мережі, правові аспекти кібербезпеки тощо. Модульна структура навчання дає можливість вивчити конкретні теми в обраному темпі і з фокусом на найбільш важливе для студента їх майбутньої кар'єри.

Враховуючи швидкість змін у галузі кібербезпеки, **гнучкі курси** , які можуть оновлюватися в реальному часі з новими загрозами та технологіями, стають все більш популярними. Наприклад, такі курси можуть включати в себе не тільки базові принципи, а й адаптацію до нових загроз, таких як атакуючі методи для хмарних систем або кіберзагрози для мобільних платформ.

З огляду на глобалізацію освіти та розвиток онлайн-навчання, важливу роль виконують **онлайн-платформи для навчання** . Використання таких платформ, як **Coursera** , **Udemy** , **edX** дає можливість студентам навчатися з будь-якої точки світу, отримуючи доступ до курсів, розроблених провідними університетами та організаціями в галузі кібербезпеки.

Ці курси можуть включати лекції, відео, інтерактивні тести, завдання для самостійної роботи та форуми для обговорення. Багато курсів пропонує сертифікацію, яка може бути корисною для здобувачів освіти, щоб підтвердити свої знання на міжнародному рівні.

Навчання інформаційної безпеки для здобувачів професійної освіти потребує постійного вдосконалення навчальних програм та методів викладання, щоб забезпечити високий рівень підготовки фахівців, здатних ефективно реагувати на сучасні загрози в кіберпросторі. Враховуючи виклики, що постають перед освітою в галузі інформаційної безпеки, є кілька напрямків, у яких можна вдосконалити навчальний процес, зробивши його більш ефективним, актуальним і практично орієнтованим.

Одним з ключових аспектів є **розробка нових навчальних програм та курсів**, що відповідають актуальним вимогам ринку праці та сучасним кіберзагрозам. Для цього необхідно враховувати новітні технології, інструменти та методи, які використовуються для захисту інформації в різних середовищах — від класичних комп'ютерних систем до мобільних пристроїв, хмарних платформ і Інтернету речей. Програми повинні включати як теоретичні знання, так і практичні навички, які дозволяють студентам вивчати реальні сценарії та вчитися працювати з новими загрозами. Важливо, щоб навчальні курси охоплювали всі рівні безпеки, включаючи захист від вірусів і шкідливих програм, захист мереж, а також правові та етичні аспекти кібербезпеки.

Впровадження інтерактивних і практико-орієнтованих методів навчання є ще одним важливим кроком для покращення ефективності навчання. Студенти повинні не тільки вивчати теоретичні матеріали, а й отримувати практичні навички у використанні сучасних інструментів безпеки. Це можна досягти через використання віртуальних лабораторій, симуляцій та тренажерів, які дозволяють студентам працювати з реальними інструментами для тестування на проникнення, моніторингу безпеки та шифрування даних. Віртуальні лабораторії, на яких студенти можуть вивчати кіберзагрози та активно працювати з ними, дають можливість реалізувати навчання в безпечному середовищі, не ризикуючи реальними інформаційними системами.

Створення умов для практичного застосування знань у реальних умовах є критичним для підготовки кваліфікованих фахівців з інформаційної безпеки. Для цього важливо запровадити більше стажувань, практик і проектних завдань, де студенти можуть працювати над реальними кейсами. Це дозволить їм не тільки поглибити теоретичні знання, а й набратися досвіду роботи з реальними кіберзагрозами та системами безпеки. Співпраця з реальними підприємствами та організаціями, де студенти можуть брати участь в реальних проектах з кібербезпеки, стане чудовим способом забезпечити практичну орієнтацію навчання.

Важливою складовою також є підвищення кваліфікації викладачів, оскільки ефективність навчання значною мірою залежить від досвіду і знань викладачів. Зважаючи на швидкий розвиток кіберзагроз і технологій, необхідно постійно оновлювати курси для викладачів, організовувати для них тренінги, семінари і вебінари, щоб вони були в курсі останніх змін у галузі кібербезпеки. Водночас важливо, щоб викладачі мали можливість працювати з новітніми інструментами та програмами, що використовуються для забезпечення інформаційної безпеки.

Оновлення методичних матеріалів та навчальних засобів також є важливим аспектом. Сучасні навчальні матеріали мають бути інтерактивними і орієнтованими на практичну діяльність. Це включає створення відеоуроків, онлайн-курсів, тестів, інтерфейсів для симуляцій, що дозволяють студентам самостійно навчатися та тестувати свої знання. Вони мають бути структуровані таким чином, щоб студенти могли починати з базових тем і поступово переходити до більш складних завдань, що дозволить забезпечити ефективне засвоєння матеріалу.

Не менш важливим є також **розвиток співпраці між навчальними закладами, державними органами та приватним сектором**, що дозволяє створювати інноваційні програми, курси і сертифікаційні системи, які забезпечують відповідність стандартам міжнародних організацій у галузі кібербезпеки. Так, міжнародні сертифікації, такі як CISSP, CEH, CompTIA

Security+, дозволяють студентам отримати додаткові кваліфікації, які будуть корисними для їх майбутньої кар'єри.

Враховуючи всі ці рекомендації, можна значно покращити навчання інформаційної безпеки та підготувати висококваліфікованих фахівців, здатних протистояти сучасним кіберзагрозам. Важливо створювати систему, де теорія безпеки органічно поєднується з практикою, де студенти мають можливість не тільки освоїти основи, а й набути реального досвіду, працюючи з актуальними загрозами та захистом інформаційних систем у реальному часі.

2.2 Інформаційна безпека здобувачів професійної освіти в інтернет мережі

Однією з головних проблем для вчителів та батьків є неконтрольованість Інтернету як джерела інформації, інформації та даних. Тому що у глобальній комп’ютерній мережі є багато матеріалів, які не тільки не є корисними для здобувачів професійної освіти, а й можуть завдати шкоди їх психічному, моральному чи навіть фізичному здоров’ю.

Для захисту здобувачів професійної освіти від психологічного, морального та фізичного насильства в Інтернеті, а також загроз і викликів, які несе з собою сучасний інформаційний простір, необхідна співпраця сім’ї та загальноосвітніх навчальних закладів, особливо в питанні навчання здобувачів професійної освіти навичкам безпечної праці з інформацією в Інтернеті [34].

Одним із шляхів забезпечення інформаційної безпеки здобувачів професійної освіти є організація захищеного персонального інформаційного простору як у закладі освіти, так і в сім’ї. Організувати захищений інформаційний простір можливо шляхом впровадження засобів і заходів забезпечення інформаційної безпеки здобувачів професійної освіти, у тому числі: правових, техніко-програмних, навчально-організаційних, морально-етичних [35, С.75].

Інформаційна безпека здобувачів професійної освіти в Інтернет-мережі є важливою складовою частиною навчального процесу в умовах стрімкого розвитку цифрових технологій. Інтернет-став основним засобом для обміну інформацією, навчання, проведення і навіть досліджень для соціалізації студентів. Однак із зростанням використання Інтернету зростають і загрози, що залишають під сумнів безпеку особистої інформації та даних здобувачів освіти. Таким чином, забезпечення інформаційної безпеки студентів у цифровому середовищі є затребуваністю, яка включає як захист персональних даних, так і безпеку процесу навчання.

2.2.1. Загрози інформаційній безпеці здобувачів освіти в Інтернеті

Інтернет-мережа є джерелом безлічі загроз для інформаційної б

- **Фішинг** : одна з найбільш розширених форм шахрайства, що забезпечує отримання доступу до особистих даних через підроблені веб-сайти, електронні листи чи повідомлення.
- **Шкідливе програмне забезпечення (malware)** : віруси, трояни, черв'яки та програми-вимагачі, які можуть прикрасити особисту інформацію, пошкодити систему або зашкодити роботі комп'ютера.
- **Атаки "людина посередині" (MITM)** : де зловмисник перехоплює або змінює комунікацію між студентом і навчальним закладом, отримуючи доступ до конфіденційної інформації.
- **Соціальна інженерія** : маніпуляції людьми для отримання доступу до особистих даних або систем, включаючи те, що обман або психологічний тиск на студентів.
- **Атаки на мережу Wi-Fi** : незахищені мережі Wi-Fi можуть бути використані для несанкціонованого доступу до даних користувачів, що особливо актуально для студентів, які часто використовуються загальнодоступними мережами в університетах, бібліотеках або кафе.

2.2.2. Методи захисту інформаційної безпеки в Інтернеті для здобувачів освіти

Для захисту своїх даних у мережі Інтернет студенти повинні використовувати кілька основних заходів:

- **Використання надійних паролів** : важливо вибирати складні, унікальні паролі для кожного онлайн-аккаунта, які важко здогадатися зловмисникам. Крім того, використання двофакторної автентифікації досягає значного рівня безпеки.
- **Антивірусне програмне забезпечення** : наявність актуальних антивірусних програм є необхідним для захисту від шкідливих програм і вірусів, які можуть пошкодити систему або покрасити особисті дані.
- **Шифрування даних** : використання шифрування при передачі даних через Інтернет (наприклад, за допомогою SSL/TLS) забезпечує їх конфіденційність. Важливо також шифрувати особисті файли і документи.
- **Безпечне використання Wi-Fi** : студентам слід відключити підключення до відкритих, незащищених мереж Wi-Fi або використовувати віртуальні приватні мережі (VPN), щоб забезпечити безпеку під час роботи в Інтернеті.
- **Оновлення програмного забезпечення** : повільне оновлення операційної системи та програмне забезпечення захистити комп’ютер від відомих вразливостей, які можуть бути використані зловмисниками.
- **Використання онлайн-сервісів для зберігання файлів** : для запобігання втраті важливих даних студенти повинні використовувати хмарні сервіси, які забезпечують захист даних і надають можливість зберегти їх у зашифрованому вигляді.

2.2.3. Роль освітніх закладів у забезпеченні інформаційної безпеки студентів

Освітні заклади мають важливу роль у формуванні знань і навичок студентів з інформаційної безпеки. Вони не повинні лише забезпечувати

технічний захист своїх інформаційних систем, але й впроваджувати навчальні програми, які охоплюють основи цифрової безпеки для здобувачів професійної освіти:

- **Навчання основам інформаційної безпеки** : студенти повинні вивчати основи кіберзахисту, включаючи безпечне користування Інтернетом, захист особистих даних, основи криптографії та роботи із захищеними з'єднаннями.
- **Підвищення обізнаності щодо кіберзагроз** : навчальні заклади мають організовувати тренінги, семінари та інформаційні кампанії для студентів, щоб підвищити їх обізнаність про існуючі загрози та методи захисту.
- **Впровадження політики безпеки** : університети повинні створювати політики безпеки для своїх онлайн-ресурсів, включаючи контроль доступу до студентських облікових записів, захист даних на серверних системах і безпеку Wi-Fi мережі.
- **Інформаційна підтримка** : заклади освіти можуть створити гарячі лінії для студентів, на яких вони можуть отримати допомогу в разі порушення безпеки або загрози безпеки.

2.3 Комплекс заходів для захисту здобувачів професійної освіти від інформаційних загроз

Політика інформаційної безпеки, що стосується здобувачів професійної освіти професійно-технічної освіти, має бути розроблена в кожному навчальному закладі та встановлена у вигляді правил ІБ (див. Додаток Б). Зазначаємо, що основними принципами політики безпеки мають бути: послідовність, обов’язковість, злочинність[31].

Необхідні заходи захисту від навмисних і ненавмисних дій здобувачів професійної освіти ПТНЗ: контроль з боку викладача, персоналізація та

обмеження доступу до критичних ресурсів, контроль і реагування на несанкціоноване використання засобів захисту програмного забезпечення, реагування персоналу, викладача та застосування відповідних педагогічних заходів. .

Основна мета політики безпеки полягає в тому, щоб переконатися, що користувачі професійного навчання дотримуються правил інформаційної безпеки, які запобігають або мінімізують шкоду, яку вони можуть завдати своїми діями, навмисними чи ненавмисними, компоненту програмного забезпечення. Ця мета досягається за допомогою організаційних, апаратно-програмних та педагогічних заходів.

Комплексний підхід до інформаційної безпеки передбачає поєднання таких заходів щодо користувачів професійної освіти: контроль з боку викладача (переважно візуальний), контроль і реагування на несанкціоновані дії засобів захисту програмного забезпечення, реагування персоналу у разі виникнення та застосування. відповідних виховних заходів. Під несанкціонованими ми маємо на увазі дії, які заборонені політикою безпеки та вказані в правилах користувача[31].

Організаційні заходи передусім включають розробку, впровадження та моніторинг реалізації політики інформаційної безпеки щодо користувачів, які проходять професійне навчання. Контроль за виконанням несуть викладачі та обслуговуючий персонал.

Особливої уваги потребує проблема доступу до Інтернету. Правила доступу до Інтернету, встановлені в закладі професійної освіти, мають бути формалізованими, тобто мати форму обов’язкового документа. Як свідчить світовий досвід, можливою формою цього документа є письмова угода, підписана учнями ПТНЗ, їхніми батьками та викладачем, яка визначає порядок користування Інтернетом, тобто приймає формалізовані правила для Інтернету «колективного договору». Ці Правила обов’язково повинні містити вказівки щодо оприлюднення в мережі Інтернет персональних даних здобувачів професійно-технічної освіти, їх фото, аудіо- та відеоматеріалів тощо.

Частина положень політики безпеки щодо доступу до Інтернету для студентів професійно-технічного навчання має бути повідомлена до початку відповідних курсів. Найкращий варіант, коли вчитель бере на себе роль порадника, а не керівника. Цього можна спробувати досягти, провівши з дітьми бесіду, в якій їм детально розкажуть про шкідливість Інтернету. Треба навчити їх виходити з неприємних ситуацій. Їм слід пояснити, як безпечно користуватися Інтернетом, перш ніж їм буде надано доступ до Інтернету або окремих електронних адрес. Наприкінці розмови поясніть та обговоріть обмеження щодо використання Інтернету. Набагато простіше підвищити безпеку, користуючись Інтернетом разом.

Апаратно-програмне забезпечення прийнятої політики безпеки реалізується системою управління (системою контролю) доступу користувачів до ресурсів, яка включає ідентифікацію та автентифікацію користувачів, керування (контроль) доступом до ресурсів, а також журналювання та аудит дій користувачів. Програмно-технічні засоби повинні забезпечувати захист критично важливих компонентів системи від несанкціонованих і помилкових дій користувача. У правилах виключення доступу необхідно заборонити цим користувачам доступ до системних областей жорсткого диска, а також модифікацію програмного забезпечення, навчальної та іншої важливої інформації. Доступ до мережі Інтернет рекомендується надавати лише з комп’ютерів, які постійно перебувають у полі зору вчителя. Варто також використовувати програми, які дають змогу відображати вміст екранів усіх комп’ютерів на моніторі викладача, тим самим відстежуючи діяльність здобувачів професійної освіти ПТНЗ [31].

Виховні заходи мають принципове значення для реалізації політики безпеки. Тому що вони служать як для запобігання несанкціонованим діям, так і для впливу на порушення правил безпеки з метою їх перевиховання. Дуже важливо встановити правила покарання тих, хто зловживає доступом. Порушення можуть бути не такими серйозними, але їх потрібно обговорювати і передбачати серйозні покарання за серйозні порушення.

Не слід забувати, що основним завданням професійно-технічного навчального закладу є виховання майбутнього громадянина. З кожним роком зростає кількість працівників, які так чи інакше використовують інформаційні технології у своїй повсякденній роботі. Крім того, немає сумніву, що роль інформаційної безпеки як невід'ємної частини будь-якої інформаційної системи зростає. Найбільш вразливою ланкою будь-якої системи безпеки були і залишаються люди. Тому майбутнє кваліфікованого працівника неможливо уявити без необхідних базових знань з інформаційної безпеки. Велику роль відіграє не лише освіта, а й виховання, адже лише воно забезпечує засвоєння морально-етичних норм у сфері інформаційних технологій.

Політика безпеки при роботі з користувачами, які є студентами професійно-технічної освіти, і з педагогічної точки зору повинна сприяти вихованню студентів професійно-технічної освіти, особливо винагороджуючи хорошу поведінку (розширюючи права) і «покараючи» погану поведінку. Основними способами безумовної реалізації політики безпеки користувачами є інформування, контроль, запит, попередження, тимчасове блокування (відмова в доступі), обмеження наданих прав і привілеїв (як користувача) та інші [31].

Основна мета навчальної діяльності – усвідомлення учнями ПТНЗ відповідальності за свої вчинки навіть у «віртуальному» середовищі, засвоєння етичних норм поведінки в цьому середовищі, що призводить до формування компетентності у сфері інформаційної безпеки у ПТНЗ. освіта[36].

Висновки до розділу 2

1) У сучасному цифровому світі забезпечення інформаційної безпеки є невід'ємною складовою професійної підготовки фахівців. З огляду на зростання кіберзагроз та необхідність захисту персональних і конфіденційних даних, важливо, щоб здобувачі професійної освіти отримували систематичну підготовку з інформаційної безпеки. Це допоможе їм не лише ефективно працювати з інформаційними системами, але й забезпечувати належний рівень захисту на усіх етапах взаємодії з інформацією.

2) Одним із найбільш ефективних підходів до навчання є інтерактивні методи, які сприяють більш глибокому розумінню та засвоєнню матеріалу. Використання віртуальних лабораторій, симуляційних платформ, кейс-стаді, а також рольових ігор дозволяє студентам не лише теоретично ознайомлюватися з проблемами інформаційної безпеки, а й отримувати практичний досвід в умовах, наближених до реальних загроз. Це дозволяє забезпечити більш глибоке і стійке засвоєння навичок захисту інформаційних систем.

3) Практична складова навчання є критично важливою для підготовки висококваліфікованих фахівців у сфері інформаційної безпеки. Використання реальних інструментів для тестування на проникнення, моніторингу безпеки, виявлення вразливостей і криптографії забезпечує студентам навички, які вони зможуть використовувати в реальній практиці. Платформи для симуляцій, такі як TryHackMe чи Hack The Box, надають студентам можливість працювати з реальними сценаріями, де вони можуть без ризику для реальних систем випробовувати свої знання та розвивати практичні навички.

4) Навчальні програми повинні бути динамічними і адаптивними до швидко змінюваного світу кібербезпеки. Враховуючи постійно зростаючі загрози і нові методи атак, необхідно регулярно оновлювати матеріали курсів, включати в навчальні програми новітні технології захисту, методи виявлення загроз і реагування на інциденти. Важливо також орієнтувати навчання на

роботу з новими технологіями, такими як хмарні обчислення, Інтернет речей, штучний інтелект і блокчейн.

5) Викладачі повинні бути не лише експертами у своїй галузі, але й мати актуальні знання з інформаційної безпеки, враховуючи останні тенденції в кіберзагрозах та методах захисту. Для цього викладачі повинні регулярно проходити професійне навчання, участь у семінарах, тренінгах і конференціях, де вони можуть обмінюватися досвідом та оновлювати свої знання з кібербезпеки.

6) Важливо, щоб студентам надавалася можливість застосовувати отримані теоретичні знання на практиці через проекти, стажування та інші форми навчання. Це дозволяє студентам не лише глибше засвоїти матеріал, а й навчитися вирішувати реальні проблеми в галузі кібербезпеки, готуючи їх до майбутньої професійної діяльності.

7) Для ефективного навчання інформаційної безпеки важливо забезпечити безпеку самої навчальної системи. Це включає впровадження заходів для захисту студентських даних, використання безпечних платформ для онлайн-навчання, захист від кібератак на навчальні ресурси та підтримку політики конфіденційності.

РОЗДІЛ 3. РЕАЛІЗАЦІЯ ПІДГОТОВКИ ЗДОБУВАЧІВ ПРОФЕСІЙНОЇ ОСВІТИ ДО ДОТРИМАННЯ ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Як видно з аналізу тенденцій розвитку суспільства, наслідків переходу до постіндустріальної економіки, реалій інформатизації освітніх і професійно-технічних закладів зокрема, темпів розвитку комп'ютерних технологій та завдань Професійна діяльність учителя інформатики проходить у наш час чітко. Вчитель інформатики все частіше отримує завдання інженера з інформаційних та комунікаційних технологій (ІКТ). Він має не лише викладати предмет інформатики, а й підтримувати працездатність апаратного та програмного забезпечення шкільного комп'ютерного класу. На цьому фоні виникає потреба ввести курс з інформаційної безпеки (ІБ) у зміст підготовки майбутніх викладачів ІТ. Ми зазначаємо, що під інформаційною безпекою ми маємо на увазі «... заходи, вжиті для запобігання несанкціонованому або зловмисному використанню, зміні або відмові в доступі до інформації, фактів, даних або обладнання» [37].

3.1 Задачі професійної діяльності викладача інформатики з інформаційної безпеки

Розберемо типові завдання вчителя інформатики з інформаційної безпеки в умовах професійного навчального закладу. Основним завданням є проектування, розвиток і вдосконалення існуючої системи безпеки інформаційної системи школи. Тому, спираючись на знання методики створення типової системи захисту (така методика має входити до змісту курсу інформаційної безпеки), вчитель інформатики повинен вміти її проектувати, розробляти та впроваджувати відповідно до фактичної вимоги, технічні можливості та наявне програмне забезпечення. Це завдання вимагає комплексного системного підходу, технічних знань, а також знань і навичок з основних питань ІБ, рівень яких повинен відповідати вимогам захисту типової

системи. Важливу роль відіграє також позитивна мотивація вчителя та переконання в необхідності такого захисту.

Завдання проектування, розробки та впровадження типової системи захисту можна віднести до розвивального виду професійної діяльності вчителя інформатики. Учитель інформатики організовує освітню діяльність в середовищі професійного навчального закладу. Програмний компонент цього середовища найбільш вразливий до навмисного чи ненавмисного втручання. Враховуючи вікові психологічні особливості ПТНЗ та рівень їх навчальних досягнень, а також дбайливе використання комп'ютерної техніки, викладач повинен організувати захист важливої інформації та критичних компонентів програмного забезпечення від втручання. Через систему заборон та ієрархічного доступу до інформації необхідно формувати у здобувачів професійного навчання свідоме ставлення до комп'ютерних пристроїв і програмного забезпечення, а також до інформації як фактора ризику. Мета полягає в тому, щоб сприяти повазі до цих речей шляхом зміни повноважень, наданих студенту як користувачу, беручи до уваги його вік, рівень його дисципліни та його знання. Крім того, свою роль може зіграти створення системи індивідуальних паролів і системи реєстрації та відстеження несанкціонованих дій користувачів, які проходять професійну підготовку. Віднесемо це типове завдання до організаційно-управлінської діяльності вчителя інформатики[37].

Перед учителем інформатики також стоїть завдання підвищення правової культури здобувачів професійної освіти в питаннях захисту конфіденційності інформації та захисту інтелектуальної власності (програмних продуктів). Стрімке поширення комп'ютерної залежності серед дітей та здобувачів професійної освіти ПТНЗ вимагає підвищення рівня знань учителів інформатики з психології та педагогіки. Необхідно, щоб вчитель інформатики консультував і підтримував батьків з питань, пов'язаних з цією проблемою.

Враховуючи розширення змісту діяльності вчителя інформатики, необхідність подальшого розвитку його компетенції, пов'язаної з наданням інформаційно-консультативних послуг вчителям, батькам, здобувачам професійної освіти, а також широке розповсюдження домашніх ПК, Необхідно розвивати їхнє вміння інформувати батьків про необхідність переконання захистити дітей від шкідливої інформації. Необхідність консультування батьків щодо можливостей програмно-технічної реалізації для запобігання доступу дітей до шкідливої інформації через домашній ПК вимагає від майбутніх учителів набуття необхідної компетенції з інформаційної безпеки. Ці типові завдання є корисним доповненням до культуропедагогічної роботи вчителя інформатики в галузі інформаційних технологій[37].

З метою розширення змісту курсу інформатики кожен випускник загальноосвітнього професійно-технічного навчального закладу повинен мати базові знання з інформаційної безпеки. Це типове завдання є частиною педагогічної роботи вчителя інформатики ІТ-сектору. Освітні завдання у сфері інформаційної безпеки передбачають, насамперед, формування у здобувачів професійної підготовки таких установок, установок і переконань:

- критичне ставлення до інформації, розвиток критичного мислення;
- свідоме ставлення до інформації як до власності;
- свідоме поводження з інформацією як фактор ризику;
- Звернення до ЕОМ як до засобу виробництва;
- дбайливе використання програмно-технічного забезпечення шкільного класу;
- Віра в необхідність захисту своєї електронної інформації.

Основною метою навчання у сфері інформаційної безпеки є формування якостей особистості, характеру здобувачів професійного навчання, які забезпечують самозахист молодої людини від загроз інформаційного середовища. Ці типові завдання конкретизують педагогічну функцію вчителя інформатики щодо захисту інформації.

Слід акцентувати увагу на особистих якостях випускника ВНЗ, необхідних для успішної реалізації компетентності інформаційної безпеки у професійній діяльності викладача. Вони стосуються загальних ключових компетенцій. Це лідерська дисциплінованість, наполегливість, ініціативність, комунікабельність та бажання професійно розвиватися.

Тому необхідно доповнити зміст професійної підготовки майбутніх учителів ІТ курсом з інформаційної безпеки, адаптованим до педагогічних предметів. Подальших досліджень потребує з'ясування умов ефективного формування компетентності майбутнього вчителя інформатики у сфері захисту інформації.

3.2 Методика забезпечення безпеки здобувачів професійної освіти у навчальному процесі

Забезпечення інформаційної безпеки здобувача професійної освіти – це комплекс взаємопов'язаних заходів, засобів і методів захисту, спрямованих на досягнення стану захищеності життєво важливих інтересів особи в комп'ютерно-орієнтованому освітньому середовищі. Обов'язковою умовою забезпечення інформаційної безпеки здобувачів професійної освіти є створення безпечного комп'ютерно-орієнтованого навчального середовища.

Важливою темою є визначення питань інформаційної безпеки студента, тобто тих, хто відповідає за забезпечення цієї безпеки. Проаналізувавши науково-методичну літературу, встановлено, що модель забезпечення комплексної інформаційної безпеки в професійному навчальному закладі [38], а також модель системи інформаційної безпеки навчального комп'ютерного комплексу [39] можуть слугувати як модельні основи організації інформаційної безпеки в навчальному закладі. На основі зазначених моделей можна розподілити відповідальність персоналу за виконання відповідних видів діяльності та визначити ієрархію управління системою комплексної

діяльності ІБ. Аналіз об’єктів та суб’єктів забезпечення інформаційної безпеки в державній освіті дозволяє виділити основних суб’єктів забезпечення інформаційної безпеки здобувачів професійної освіти , а саме: сам учень, учитель інформатики, вчителі-предметники, технічний персонал та дирекція ПТНЗ.

На думку М. І. Бочарова: «Провідна роль у забезпеченні та навчанні ІБ у середньому загальноосвітньому навчальному закладі належить вчителю інформатики, який зможе навчати та забезпечувати комплексне ІБ у середньому загальноосвітньому навчальному закладі» [38].

Завдання вчителя інформатики – організувати захист інформаційних ресурсів, навчального комп’ютерного комплексу та здобувачів професійної освіти від найімовірніших інформаційних загроз та негативних наслідків ІКТ. Це дозволяє сформулювати таке визначення. Професійна компетентність учителя інформатики у сфері інформаційної безпеки – це сукупність знань і розуміння, умінь, навичок, а також особистісних установок і ціннісних орієнтацій учителя у сфері інформаційної безпеки та здатність самостійно та відповідально здійснювати інформаційну безпеку. демонструвати їх у розв’язанні типових професійних завдань та розв’язанні проблем інформаційної безпеки, що виникають у реальних умовах навчального процесу ПТНЗ [40].

Методика забезпечення безпеки здобувачів професійної освіти в навчальному процесі є надзвичайно важливою, оскільки навчальний процес, особливо в умовах цифровізації, містить численні ризики, пов’язані з використанням інформаційних технологій. Зростання кіберзагроз, захист персональних даних, а також наявність потенційних загроз під час взаємодії з навчальними системами й ресурсами ставлять завдання забезпечення безпеки студентів як пріоритет.

Основним завданням методики є формування у студентів знань і навичок, що дозволяють їм безпечно працювати з технологіями, даними і цифровими системами, а також розуміння важливості захисту особистої та

академічної інформації. Це охоплює багато аспектів, від правових аспектів захисту персональних даних до технічних заходів безпеки в навчальних системах.

В першу чергу, методика повинна включати навчання основам кібербезпеки для студентів, що забезпечить базову обізнаність про загрози та методи їх захисту. Це має бути включено в основну навчальну програму, де студенти вивчають не лише теоретичні аспекти безпеки, а й практичні навички, як наприклад, налаштування надійних паролів, безпечне використання Інтернету, захист від фішингу, використання віртуальних приватних мереж (VPN) та антивірусних програм. Важливо навчити студентів не лише захищати свої особисті дані, але й працювати з іншими людьми, коли мова йде про захист даних організації чи навчального закладу.

Другим важливим аспектом є створення безпечних умов для доступу до навчальних ресурсів. Це включає захист платформ для дистанційного навчання, серверів, на яких зберігаються академічні дані, а також забезпечення безпеки при використанні хмарних технологій для зберігання та обміну документами. В умовах пандемії та переходу на дистанційне навчання цей аспект став ще більш актуальним, оскільки навчальні заклади змушені покладатися на онлайн-платформи для проведення лекцій, здачі іспитів і передачі матеріалів.

Крім того, важливо створювати чіткі правила користування мережами і програмними засобами в межах навчального закладу. Зазвичай для цього в організаціях розробляють політики безпеки, що регулюють доступ до інформаційних ресурсів, використання електронної пошти, а також правила поведінки у разі виявлення кіберзагроз або інцидентів. Такі політики повинні бути доступні для всіх учасників навчального процесу, а також регулярно оновлюватися з урахуванням нових викликів і загроз у сфері інформаційної безпеки.

Важливою частиною методики є також підготовка викладачів. Вони повинні не лише володіти спеціальними знаннями з відповідних предметів, а

й бути обізнаними з основами кібербезпеки, мати навички роботи з сучасними навчальними інструментами та платформами, а також володіти інструментами для запобігання витоку даних або несанкціонованого доступу до систем. Для цього необхідно організувати регулярні тренінги і семінари для педагогів, де вони можуть здобути знання про новітні загрози, методи їх виявлення та нейтралізації.

Не менш важливою складовою є забезпечення захисту прав студентів, особливо в контексті персональних даних. У відповідності до законодавства про захист даних, навчальні заклади повинні забезпечити відповідну політику щодо зберігання, обробки та захисту персональних даних студентів. Це включає захист особистої інформації від несанкціонованого доступу, а також забезпечення безпеки онлайн-тестувань, захисту результатів навчання та індивідуальних робіт.

Загалом, методика забезпечення безпеки здобувачів професійної освіти в навчальному процесі є багатогранним завданням, яке вимагає комплексного підходу. Це охоплює як технічні, так і правові заходи, включаючи навчання студентів, підготовку викладачів, створення безпечного інформаційного середовища в навчальних закладах і постійне вдосконалення політик і процедур безпеки. Враховуючи швидкий розвиток технологій і нові загрози в цифровому середовищі, важливо, щоб методика була гнучкою, адаптивною і здатною швидко реагувати на нові виклики.

Компетентність вчителя інформатики щодо забезпечення інформаційної безпеки студентів-педагогів має враховувати потреби захисту персональних даних здобувачів професійної освіти ПТНЗ, персональних комп’ютерів і власне здобувачів професійної освіти ПТНЗ від найімовірніших інформаційних загроз та негативних наслідків ІКТ. . Результатом діяльності вчителя інформатики та інших суб’єктів забезпечення інформаційної безпеки (адміністрації ПТНЗ, технічного персоналу) має бути забезпечення інформаційної безпеки всіх перерахованих вище об’єктів[40].

На функціональній моделі (рис. 3.2) розглянуто низку заходів захисту інформації, показано, які суб'єкти здійснюють ці заходи та на які характеристики старшокласника вони спрямовані. Показано, що основою формування інформаційно захищеної особистості випускника є безпека КОНС як середовища соціалізації особистості. Безпека КОНС забезпечується комплексом апаратно-програмних засобів, а також організаційними, освітніми та процедурними заходами. Метою забезпечення ІБ старшокласника є формування інформаційно захищеної особистості, яке відбувається на основі навчання та формування відповідних якостей і навичок особистості: дисциплінованості, компетентності та культури ІБ.

На підставі всіх проблем і порад, розглянутих у даній роботі, було визначено, що необхідно скласти плани уроків, оскільки дана тема включена в програми з інформатики, а також у пам'ятку для всіх здобувачів професійної освіти профтехосвіти, в якій курс читається.

З педагогічної точки зору правила інформаційної безпеки користувачів, які проходять професійну підготовку, повинні сприяти освіті тих, хто проходить професійну підготовку. Зокрема, доцільно винагороджувати (розширювати права) та «карати» тих, хто проходить професійне навчання за хорошу поведінку. «на погане. Основними методами безумовної реалізації політики безпеки користувачами є інформування, моніторинг, запит, попередження, тимчасове блокування (відмова в доступі), обмеження наданих прав і привілеїв (як користувача НКЦ) та інші[40] .

Основна мета виховної діяльності – усвідомлення здобувачами освіти відповідальності за свої дії навіть у «віртуальному» середовищі, засвоєння етичних норм поведінки в цьому середовищі і тим самим формування культури та компетентнісної інформаційної безпеки здобувачів ПТНЗ. .

Одним із завдань було створення пам'ятного блокнота (див. Додаток Б). Це повідомлення необхідно для дитини, щоб вона могла ним скористатися в будь-який час, незалежно від свого віку, і щоб дитина розуміла, що таке

інформаційна безпека, які її особливості та небезпеки, що можна робити в Інтернеті та яку інформацію (цифрові дані) можна знайти в мережі Інтернет.

У цій брошурі пояснюється, що таке інформаційна безпека та які існують заходи, що призводять до моральної чи матеріальної шкоди. Також показано правила поведінки на уроках з комп'ютера, правила захисту від вірусів та основні правила забезпечення інформаційної безпеки при роботі в мережі Інтернет.

Рекомендується вивішувати цю пам'ятку біля кожного комп'ютера в класі. Таким чином дитина може використовувати його в будь-який час.

Переходимо до розробки практичних курсів (див. Додаток В). Тема заняття: «Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті та як їх уникнути.

На цьому уроці нам необхідно визначити, що таке інформаційна безпека, розвинути вміння аналізувати інформацію (цифрові дані), визначити основні загрози інформаційній безпеці користувача Інтернету та ознайомитися з правилами безпечної роботи в Інтернеті та правилами інформаційної безпеки при роботі з комп'ютером; викликати інтерес до вивчення інформаційних технологій та розвивати економне ставлення до обладнання кабінету інформатики.

Цей урок є комбінованим, оскільки на ньому використовуються різноманітні методи та прийоми навчання, а саме: індивідуальна, групова, самостійна робота здобувачів професійної освіти ПТНЗ. Курс пропонується проводити з використанням інтерактивних технологій.

Перша частина цього уроку – визначення теми, мети та завдань. Вчитель інформатики знайомить дітей з актуальністю даного уроку.

У другій частині вчитель інформатики знайомить дітей з основними поняттями та пояснює новий матеріал. Ставить завдання на логіку та ставить завдання для самостійної роботи здобувачів професійного навчання в Інтернеті та в закладі професійної освіти. Діти мають за допомогою нетбуків

дізнаватися значення понять в Інтернеті та записувати їх у закладі професійної освіти.

Потім здобувачі професійної освіти самостійно працюють над завданням «Етапи розробки інформаційно-комунікаційних засобів». У результаті розв'язаного завдання діти повинні скласти схему, на якій відобразити етапи розвитку спілкування. Потім приступають до роботи з підручником. У ході роботи з інформацією підручника створено схему “Класифікація атак на комп’ютерні системи”.

Далі здобувачі професійної освіти повинні розділитися на три групи для виконання групового завдання. Перша група охоплює основні типи загроз, пов'язаних з особистою безпекою, безпекою інших осіб і розробкою персональних даних. Другий описує захист держави в частині забезпечення інформаційної безпеки. У третьому розділі перераховані варіанти уникнення загроз під час роботи в Інтернеті.

Наприкінці уроку закріплюються знання, підводяться конспекти та роздається домашнє завдання.

Висновки до розділу 3

1) В умовах швидкого розвитку інформаційних технологій і зростаючої кількості кіберзагроз, підготовка здобувачів професійної освіти до дотримання вимог інформаційної безпеки є важливою складовою частиною їхньої професійної підготовки. Оскільки інформаційна безпека охоплює не тільки технічні аспекти, але й правові, етичні та організаційні питання, необхідно забезпечити комплексний підхід до навчання студентів.

2) Для ефективної підготовки фахівців з інформаційної безпеки важливо, щоб навчальні програми та курси відповідали актуальним вимогам галузі. Програми повинні включати не лише базові теоретичні знання, а й практичні навички роботи з сучасними інструментами та методами захисту інформації, що дозволить студентам вільно орієнтуватися в умовах сучасних кіберзагроз.

3) Теоретичні знання повинні супроводжуватися практичними заняттями, що дозволяють студентам отримати досвід роботи з реальними інструментами та технологіями захисту інформації. Віртуальні лабораторії, симуляції атак і захисту, тестування на проникнення та інші методи практичного навчання допомагають студентам розвивати необхідні навички для роботи в реальних умовах.

4) Оскільки кіберзагрози змінюються з неймовірною швидкістю, студенти повинні бути готові до постійного оновлення своїх знань і навичок. Для цього необхідно організувати додаткові курси підвищення кваліфікації, онлайн-курси, семінари та тренінги для студентів і викладачів, щоб вони могли бути в курсі новітніх загроз та технологій захисту.

5) Викладачі повинні бути не лише експертами в своїх професійних галузях, але й володіти сучасними знаннями з інформаційної безпеки, а також мати досвід використання сучасних інструментів захисту. Це дозволяє створити навчальне середовище, яке не лише передає теоретичні знання, але й сприяє розвитку практичних навичок.

ЗАГАЛЬНІ ВИСНОВКИ

При виконанні зазначених завдань дослідження дійшли таких висновків:

1) Вивчення існуючих підходів до навчання інформаційної безпеки: Виконання цього завдання дозволяє отримати чітке розуміння поточних тенденцій у навчанні інформаційної безпеки. Це включає як традиційні методи, так і новітні інтерактивні підходи, такі як використання віртуальних лабораторій, симуляційних платформ, а також інтеграцію теоретичних знань із практичними навичками. Виявлено, що більшість навчальних програм орієнтовані на основні аспекти кібербезпеки, але часто не враховують швидко змінювані технології та нові загрози, з якими стикаються сучасні фахівці. Також виявлено, що навчальні плани часто зосереджуються на традиційних темах, таких як захист від вірусів і шкідливих програм, але недостатньо уваги приділяється новим загрозам, таким як атаки на Інтернет речей (IoT), хмарні обчислення або загрози в мобільних середовищах.

2) Аналіз програмного забезпечення та технологій, що використовуються в освітньому процесі: При виконанні цього завдання важливо вивчити сучасне програмне забезпечення та інструменти, які використовуються для навчання інформаційної безпеки, а також оцінити їх ефективність у підготовці студентів. Виявлено, що основні інструменти, такі як антивірусне програмне забезпечення, фаєрволи, системи для тестування на проникнення, криптографічні програми та платформи для вивчення кіберзагроз (наприклад, Hack The Box, TryHackMe), є важливими для формування практичних навичок у студентів. Однак, деякі навчальні заклади мають обмежений доступ до найновіших версій програм або не мають достатньої технічної інфраструктури для впровадження таких технологій, що суттєво знижує якість навчання. Важливою проблемою є також необхідність в адаптації програмного забезпечення під сучасні загрози і нові технології, зокрема для роботи з хмарними середовищами та великими даними.

3) Розробка рекомендацій щодо вдосконалення навчальних курсів і програм для фахівців цієї галузі: Виконання цього завдання допомагає сформулювати конкретні рекомендації щодо вдосконалення існуючих навчальних курсів і програм. На основі аналізу поточних підходів до навчання та інструментів було встановлено кілька ключових напрямків для покращення: по-перше, необхідно ввести більш гнучкі курси, які б дозволяли студентам навчатися за індивідуальними програмами та темпами; по-друге, важливо оновити навчальні програми, щоб вони включали новітні технології та актуальні кіберзагрози, зокрема зосереджуючись на кібербезпеці для хмарних технологій і мобільних додатків; по-третє, є необхідність впровадження більше практичних методів навчання, таких як проекти, стажування в реальних компаніях, та використання симуляційних платформ для навчання, що дозволяють студентам працювати з реальними інструментами захисту.

Загалом, виконання цих завдань дозволяє виявити слабкі місця в існуючому підході до навчання інформаційної безпеки та пропонувати шляхи їх усунення через адаптацію навчальних курсів до сучасних викликів і вимог, а також забезпечення студентів практичними навичками, необхідними для ефективної роботи в умовах швидко змінюваної цифрової середовища.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Anderson, R. (2020). Security engineering: A guide to building dependable distributed systems (3rd ed.). Wiley.
2. Bada, A., & Sasse, M. A. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? Proceedings of the European Conference on Information Systems (ECIS) 2015, 1–16.
3. Butlin J. (2017) Our common future. Journal of International Development. London, Oxford University Press,. pp. 284–287
4. Disterer, G. (2013). ISO/IEC 27001:2013: Information security management systems. Information Security Journal: A Global Perspective, 22(1), 18–29. https://doi.org/10.1080/19393555.2013.783944
5. Freeman, M. (2018). Introduction to information security: A strategic approach. Springer.
6. Henson, R., & Williams, C. (2020). Cybersecurity education: The role of pedagogy in information security education. Journal of Information Systems Education, 31(2), 161-173.
7. Higher Education in the Twenty-First Century: Vision and Action. *UNESCO on the World Conference on Higher Education* (2018). URL: http://perso.club-internet.fr/ nicol/ciret/english/charten.htm (Last accesed: 15.10.2024).
8. Krutz, R. L., & Vines, R. D. (2010). The CISSP prep guide: Mastering the ten domains of computer security. Wiley.
9. Lemos, R. (2021). An analysis of cybersecurity education trends. International Journal of Computer Science and Information Technology, 3(2), 12–24. https://doi.org/10.1016/j.jcsit.2021.02.007
10. Liedel K. (2024) Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego. Torun: Wyd-wo Adam Marszałek,. 96 s.
11. Stallings, W. (2017). Cryptography and network security: Principles and practice (7th ed.). Pearson Education.

12. Wallerstein I. (2017). Analiza systemów-światów. Wprowadzenie. Warszawa,. 160 s.
13. Warkentin, M., & Willison, R. (2009). Behavioral information security: The "human" factor. Computers & Security, 28(8https://doi.org/10.1016/j.cose.2009.04.003
14. Weaver, S., & Haggerty, L. (2019). Information security management: Concepts, practices, and frameworks. Springer.
15. Zięba R. (2021) Instytucjonalizacja Bezpieczeństwa europejskogo. Warszawa; Scholar,. 406 s
16. Беззубов Д.О. (2023) Суспільна безпека: (організаційно-правові засади забезпечення): Моногр. К.: МП,. 451 с.
17. Биков В. Ю. (2020) Сучасні завдання інформатизації освіти. *Інформаційні технології і засоби навчання*. № 1(15). Режим доступу до журн. : http://www.ime.edu-ua.net/em.html
18. Биков В.Ю. (2018) Відкрита освіта в Єдиному інформаційному просторі. *Педагогічний дискурс* : зб. наук. праць / гол. ред. І.М. Шоробура. Хмельницький : ХГПА. Вип. 7. С. 30-35.
19. Бондаренко, В. М. (2015). Інформаційна безпека в умовах глобалізації: Проблеми та перспективи. Київ: Наукова думка.
20. Варивода К. (2016) Інформаційна безпека підлітків в Інтернет мережі. *Молодий вчений*.. Т. 3, № 30. С. 365–368.
21. Гребенюк, І. М. (2019). Основи кібербезпеки та захисту інформації. Харків: ХНУРЕ.
22. Деркач, І. В. (2017). Моделювання інформаційної безпеки: Методичні аспекти (2-е вид.). Київ: Либідь.
23. Дмитренко, О. В., & Курило, О. С. (2016). Педагогічні технології в освіті з інформаційної безпеки. Збірник наукових праць Національної академії державної податкової служби України, 3, 77-85.

24.Ільченко, В. В. (2018). Використання інформаційних технологій для навчання кібербезпеці. Технічний вісник Харківського національного університету, 2, 91-95.

25. Ковальчук В. Н. (2018) Проблеми інформаційної безпеки дітей різних вікових категорій. *Комп'ютер у школі та сім'ї*. № 8. С. 58-62.

26.Ковальчук В. Н. (2019) Система інформаційної безпеки навчального комп'ютерного комплексу: метод. рекоменд. Житомир: ЖДУ. 84 с.

27. Ковальчук В. (2017). Типові задачі професійної діяльності вчителя інформатики з інформаційної безпеки. Житомир: ЖДУ ім. І.Франка.

28. Ковальчук В. (2020) Проблеми інформаційної безпеки дітей різних вікових категорій. *Комп'ютер в школі та сім'ї*.. № 8. С. 58–62.

29.Ковальчук, В. П. (2020). Інформаційна безпека у сучасному світі. Львів: Афіша.

30. Кравець Є. А. (2020) Інформаційна безпека держави. Юридична енциклопедія: в 6 т. К.: Укр. енцикл. С. 744.

31.Ліпкан В.А. (2019) Національна безпека України: навч. посіб. К.: КНТ,. 576с

32.Малишко, В. І., & Ткачук, В. В. (2020). Актуальні проблеми підготовки фахівців з інформаційної безпеки. Науковий вісник Чернівецького університету, 9, 105-110.

33.Мельник С.В. (2016) Понятійно-категоріальний апарат у системі професійної підготовки майбутніх фахівців з кібербезпеки. *Інформаційні технології і засоби навчання*.. Т. 55. №5. С. 187–197.

34.Методичні рекомендації з інформаційної безпеки навчального комп'ютерного комплексу (2019). Укл. Дем'яненко В.М., Ковальчук В.Н. К. : ІІТЗН НАПН України. 39 с.

35.Підгорна Т., Берест І. (2018) Деякі аспекти організації інформаційної безпеки здобувачів професійної освіти . *Педагогіка і психологія професійної освіти*. № 6. С. 70-78.

36. Рамський Ю.С. (2020) Інформаційне суспільство. Інформатизація освіти. *Науковий часопис НПУ імені М.П. Драгоманова*. Серія №2. Комп'ютерно-орієнтовані системи навчання : [зб. наук. праць / Редрада]. К. : НПУ імені М.П. Драгоманова,. № 7 [Електронний ресурс]. – Режим доступу : http://www.ii.npu.edu.ua/index.php?option=com_content&view=section&id=11&Itemid=64&lang=uk

37. Соловйова, Т. М. (2014). Педагогіка кібербезпеки: Використання новітніх інформаційних технологій у навчанні. Педагогічні науки: Теорія та практика, 4(38), 134-140.

38. Філософія (2023). Навч. посіб. / За заг. ред. Ю.В. Осічнюка. К.: Атіка,. 464 с.

39. Шевченко, М. В. (2015). Захист інформації: теорія і практика. Київ: Видавництво "Київська правда".

40. Шишкіна М. П. (2022) Модельний підхід у побудові комп'ютерно-орієнтованого навчального середовища. Мат-ли Міжнародної науково-практичної конференції «*Інформатизація освіти та дистанційна форма навчання: сучасний стан та перспективи розвитку*». Суми: Сум ДПУ імені А.С.Макаренка. С. 17–21.

41. Яремчук, В. О. (2016). Використання онлайн платформ для навчання основам кібербезпеки. Вісник національного університету "Львівська політехніка", 19(2), 57-63.

42. Ященко В. А. &Щуровський А. М. (2024) Національна та державна безпека : діалектика взаємозв'язку. *Державна безпека України*.. № 1. С. 19-20.

ДОДАТОК А. Приклади правил інформаційної безпеки

Правила роботи у кабінеті інформаційно-комунікаційних технологій (доповнення правилами інформаційної безпеки)

Обов'язки користувачів по реєстрації в системі:

- Для реєстрації в системі ми повинні ввести по запиту своє користувацьке ім'я (логін) та пароль;
- Якщо ви ввели некоректно пароль три рази, то ваш обліковий запис буде заблоковано, розблокувати її може лише лаборант (вчитель інформатики);
- Ви ніколи не повинні записувати свій пароль;
- Ви ніколи не повинні повідомляти будь-кому свій логін чи пароль;
- Якщо ви забули свій пароль, необхідно особисто отримати новий у лаборанта.

Робота в комп'ютерному класі:

1. Комп'ютерне обладнання та програмне забезпечення класу призначене лише для навчальних цілей і повинно використовуватися лише для цього;

2. Не можна приносити на носіях та завантажувати на жорсткі диски комп'ютерів заборонену інформацію (порнографію, що демонструє жорстокість), стороннє програмне забезпечення.

3. У класі підтримується стандартна конфігурація всіх робочих станцій, користувачам забороняється змінювати цю конфігурацію, якщо дана зміна не передбачена навчальним завданням.

Обов'язки користувача Internet:

1. Підключення школи до Інтернету повинно використовуватися лише для навчання;

2. Забороняється використання комп'ютерів шкільного класу та підключення до Інтернету для ігор, отримання та збереження забороненої

інформації (порнографії, що демонструє жорстокість), стороннього програмного забезпечення.

3. Користувачі повинні знати що комунікації Internet не є конфіденційними. Користувачі не повинні передавати по мережі інформацію, яка містить їх конфіденційну інформацію: прізвище, адреса, телефон, особисті фотографії та іншу інформацію, розголошення якої може нанести їм шкоду.

4. Користувачі не повинні завантажувати з Internet програмне забезпечення та активні компоненти web-сторінок, а всі дані що завантажуються ними з Internet повинні пройти антивірусну перевірку. Дані, що завантажуються учнями з Internet повинні бути навчального призначення і мати розмір, що не перевищує встановлений у навчальному закладі ліміт.

Контроль та дослідження мережних даних.

Керівництво школи попереджує, що воно має право досліджувати і знищувати будь-які дані, що зберігаються на комп'ютерах та мережних системах. Також введеться контроль за діями здобувачів професійної освіти : візуальний і електронний. Якщо зібрані факти будуть свідчити про порушення користувачем правил інформаційної безпеки чи законів, то вони можуть бути використані як підстава для дисциплінарного покарання.

Правила антивірусного захисту:

1. На всіх комп'ютерах встановлено антивірусне програмне забезпечення. Обов'язок користувачів полягає у сприянні заходам антивірусного захисту.

2. Користувачі повинні перевіряти всі дані при кожному їх завантажені з будь-якого джерела. Також необхідно перевіряти будь-який переносний носій перед його відкриттям на наявність вірусів.

3. Користувачі повинні сприяти оновленню антивірусних баз, а також ніколи не перешкоджати та не вивантажувати з оперативної пам'яті антивірусні програми.

4. Користувачі не повинні створювати, запускати, передавати чи демонструвати ніяких комп’ютерних кодів, які можуть нанести шкоду системам обробки даних чи інформації, що в них зберігається.

Кодекс моральної поведінки у віртуальному середовищі:

Не можна поширювати інформацію, що може містити наклеп, образу будь-якої людини за національними, расовими, статевими, фізичними та іншими прикметами.

ДОДАТОК Б. Правила роботи у кабінеті інформаційно-комунікаційних технологій

Правила поведінки в комп'ютерному класі

- *Заходьте до комп'ютерного кабінету тільки з дозволу вчителя, не поспішаючи, не торкаючись обладнання.*
- *Не вмикайте та не вимикайте комп'ютери без дозволу вчителя. Перш ніж розпочати роботу, розмістіть зошит, ручку, підручник так, щоб вони не лежали на клавіатурі чи моніторі, а також не заважали працювати на комп'ютері.*
- *Під час роботи будьте дуже уважні. Сидіть прямо, на відстані від екрана щонайменше 50– 60 см. Лінія зору має бути спрямована до центра екрана.*
- *Не торкайтеся з'єднувальних проводів та проводів живлення.*
- *Ніколи не намагайтесь самостійно усунути несправності комп'ютера. У разі появи запаху горілого, самовільного вимикання апаратури, незвичних звуків негайно повідомте про це вчителя.*
- *Працюйте за комп'ютером не більше ніж 15 хвилин поспіль. Робіть перерви для відпочинку.*

- *У разі появи різання в очах, різкого погіршення зору, болю в пальцях та кистях рук, посилення серцебиття сповістіть учителя про свій стан і за потреби зверніться до лікаря.*
- *Після закінчення роботи закрийте всі активні програми та коректно вимкніть комп'ютер.*

Правила антивірусного захисту:

- На всіх комп'ютерах встановлено антивірусне програмне забезпечення. Обов'язок користувачів полягає у сприянні заходам антивірусного захисту.

-Користувачі повинні перевіряти всі дані при кожному їх завантажені з будь-якого джерела.

- Також необхідно перевіряти будь-який переносний носій перед його відкриттям на наявність вірусів.

- Користувачі повинні сприяти оновленню антивірусних баз, а також ніколи не перешкоджати та не вивантажувати з оперативної пам'яті антивірусні програми.

- Користувачі не повинні створювати, запускати, передавати чи демонструвати ніяких комп'ютерних кодів, які можуть нанести шкоду системам обробки даних чи інформації, що в них зберігається.

Одним зі шляхів забезпечення інформаційної безпеки підлітків є організація безпечного особистісного інформаційного простору як у школі, так і в сім'ї

Основні правила забезпечення інформаційної безпеки при роботі в інтернеті:

- *Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.*

- *Встановлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери. Бажано, щоб оновлення антивірусних баз здійснювалося регулярно та автоматично.*
- *Завжди встановлюйте оновлення операційної системи та іншого програмного забезпечення.*
- *Використовуйте надійні паролі. Не використовуйте на різних інтернет-ресурсах один і той самий пароль, змінюйте його регулярно.*
- *Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані (дані кредитних карток, онлайн-банкінгу тощо) через публічні та незахищені Wi-Fi-мережі.*
- *Установіть фільтр спливаючих вікон у браузері.*
- *Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера.*
- *Не відкривайте повідомлення електронної пошти від невідомих вам осіб і прикріплені до них файли, яких ви не очікуєте.*
- *Подумайте про можливі ризики для вас перед тим, як викласти щось у мережу Інтернет.*
- *Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.*

ДОДАТОК В. Розробка заняття на тему «Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті і їх уникнення»

Тема: «Проблеми інформаційної безпеки. Загрози при роботі в Інтернеті і їх уникнення».

Мета: формувати компетентності: *предметні* (*інформаційної культури та інформативної компетентності)***реалізація творчого потенціалу, соціалізація у суспільстві, ефективне використання засобів сучасних інформаційно-комунікаційних технологій; ***ключові компетентності:*** визначати основне поняття «інформаційна безпека», формувати вміння аналізувати інформацію, визначати основні загрози інформаційної безпеки користувача Інтернету, ознайомити здобувачів професійної освіти з правилами безпечної роботи в Інтернеті та правилами інформаційної безпеки при роботі з комп'ютером; розвивати особистісно – смислового ставлення до навчального предмета, розвиток пам'яті, логічного мислення, предметного сприйняття, уваги; виховувати інтерес до вивчення інформаційних технологій, формування бережливого ставлення до обладнання комп'ютерного кабінету.

Методи навчання, прийоми: вправа «Зірка», індивідуальна, групова, самостійна робота здобувачів професійної освіти , робота з електронним підручником, прийом «Відкрита трибуна», метод «Ланцюжок», тестування за допомогою « My Test Student».

Основні терміни і поняття: інформаційна безпека, конфіденційність, цілісність, доступність, хакерська атака, критичне мислення, спам, фішинг, шкідлива програма.

Технічні засоби навчання: персональні комп'ютери.

Програмне забезпечення: OCWindows, мережа Інтернет, браузер.

Хід заняття

I. Формулювання теми, мети й завдань, мотивація навчальної діяльності.

Слово викладача: мережа Інтернет – одне з найвидатніших винаходів людства. Завдяки світовій павутині можна навчитися, шукати за допомогою електронних пошукових систем реферати, електронні книги, енциклопедії, здійснювати покупки, не витрачаючи час на походи до магазину. Інтернет для багатьох став засобом спілкування та зв'язку. Підключивши до персонального комп'ютера чи ноутбука веб-камеру, мікрофон та колонки, можна безкоштовно спілкуватися з людиною з іншого куточка світу та ще до того ж бачити співрозмовника на моніторі. Комп'ютерна мережа часто заповнює довкілля користувачів онлайн – фільмами, телебаченням та іграми.

Віртуальні подорожі, які кожен із вас здійснює, здавалося б не можуть загрожувати якимись серйозними небезпеками. Але ваша спокійна самотність за монітором оманлива, оскільки весь час, поки встановлене Інтернет - з'єднання, ваш комп'ютер є частиною величезної мереж і, де є і друзі, і вороги. Уберегтися від небезпеки завжди простіше, якщо знати, кого і чого боятися. Тому на цьому уроці ми розглянемо проблеми та принципи інформаційної безпеки, види загроз при роботі в Інтернеті та вимоги для дотримання інформаційної безпеки на уроках

Оголошення теми, мети та плану викладу нових знань.

II. Вивчення нового матеріалу.

Пояснення викладача:

Інформаційна безпека – стан захищеності потреб людини, суспільства та держави в інформації незалежно від внутрішніх і зовнішніх загроз.

Завдання для здобувачів освіти:

- розгадайте ребуси та визначте рівні захищеності інформаційного середовища.

(Й)

,,, і ‘  

‘ність.

Очікувана відповідь(конфіденційність)

Ці   ,,,, 

Очікувана відповідь((цілісність)

 ,,,  ,   .

*Очікувана відповідь(*доступність)

Самостійна робота здобувачів освіти.

Завдання:

- Знайдіть в Інтернеті за допомогою нетбуків значення цих понять та запишіть у зошити.

Очікувана відповідь:

Під конфіденційністю розуміють забезпечення доступу до даних на основі розподілу прав доступу, захист від несанкціонованого ознайомлення.

Доступність означає забезпечення доступу до загальнодоступних даних усім користувачам і захист цих даних від блокування зловмисниками.

Цілісність передбачає захист даних від їх зловмисного або випадкового знищення чи спотворення.

Слово викладача :Інформаційна безпека держави характеризується ступенем захищеності і, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості і т. д.) стосовно небезпечних (дестабілізаційних, деструктивних, суперечних інтересам країни тощо), інформаційним впливам, причому як до впровадження, так і до вилучення інформації.

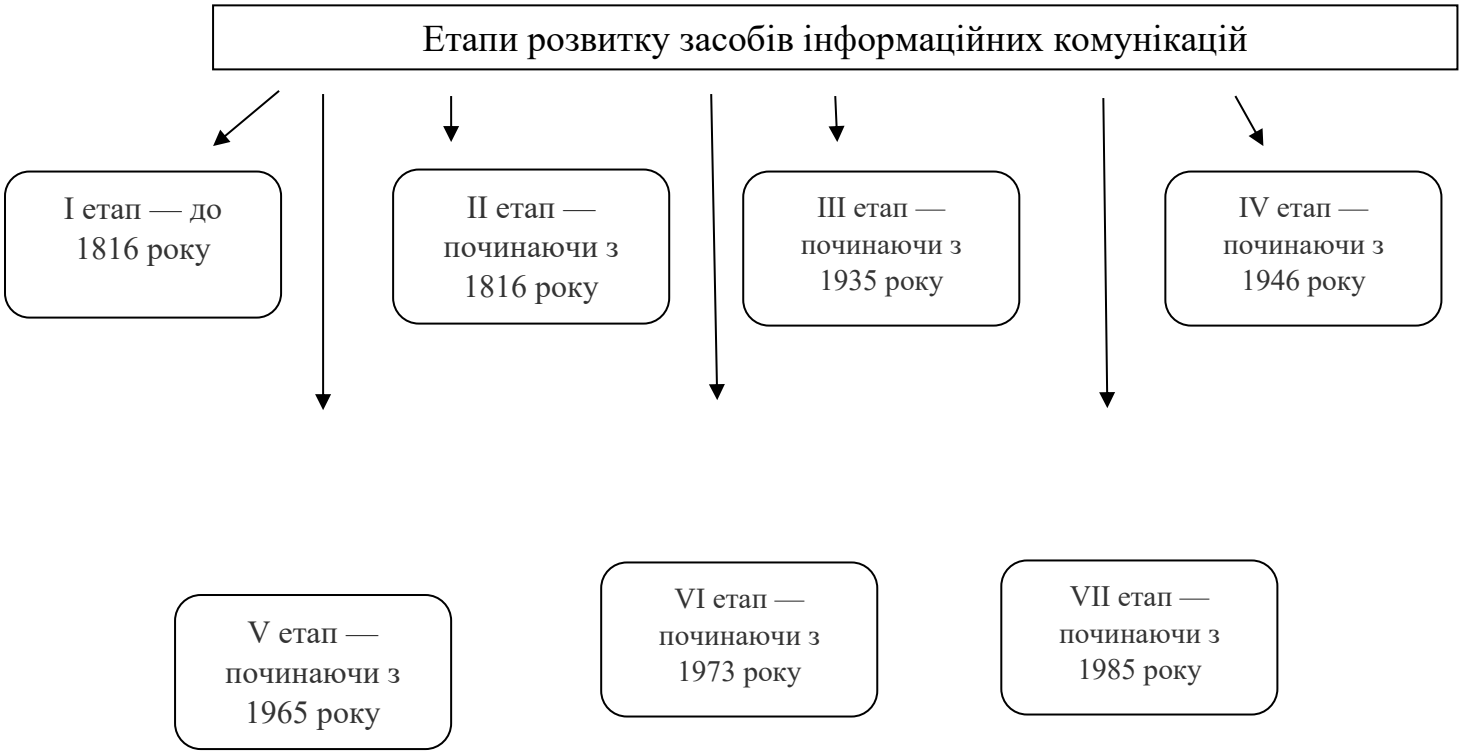
Поняття інформаційної безпеки не обмежується безпекою технічних інформаційних систем чи безпекою інформації у чисельному чи електронному вигляді, а стосується усіх аспектів захисту даних чи інформації незалежно від форми, у якій вони перебувають.

Об'єктивно категорія «інформаційна безпека» виникла з появою засобів інформаційних комунікацій між людьми, а також з усвідомленням людиною наявності у людей і їхніх співтовариств інтересів, яким може бути завдано збитку шляхом дії на засоби інформаційних комунікацій, наявність і розвиток яких забезпечує і задає інформаційний обмін між всіма елементами соціуму.

Індивідуальна робота здобувача освіти:

- Заздалегідь отримане завдання учнем «Етапи розвитку засобів інформаційних комунікацій».

Очікувана відповідь:



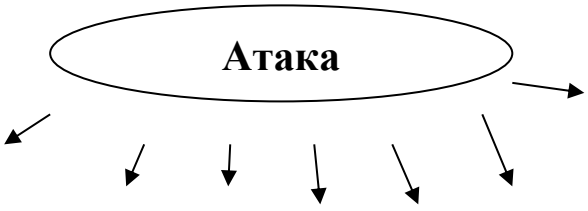
Слово викладача: Міжнародний день захисту інформації відзначається 30 листопада. З кожним роком його актуальність зростає через глобалізацію та повсюдне використання Інтернету. Сьогодні це поняття дещо трансформоване та охоплює більшу кількість проблем.

30 листопада 1988 вперше спостерігали за епідемією «хробака» («Морріс»), який показав, наскільки може бути вразливим персональний комп'ютер та інформація на ньому.

Робота з електронним підручником.

Розділ 1

- Пропоную для більш швидкої роботи з інформацією підручника скласти схему «Класифікація атак на комп'ютерні системи».



Слово викладача: Зараз в Україні майже 22 млн. користувачів Інтернету, питання безпеки в мережі більш ніж актуальне. У цьому контексті турбота про дітей набуває більших масштабів. Якщо раніше треба було говорити з дітьми про їх безпеку поза домом тощо, то вже давно має сенс застерігати їх від негараздів під час перебування в Інтернеті.

Групова робота здобувача освіти.

Завдання.

- За допомогою нетбуків, користуючись мережею Інтернет та об'єднавшись в три групи, виконайте завдання.

1 група – Запишіть основні типи загроз, які стосуються особистої безпеки, безпеки інших, розвитку персональної інформації.

2 група – Захист держави, щодо забезпечення інформаційної безпеки.

3 група – Уникнення загроз під час роботи в Інтернеті.

Слово викладача: Інформаційна безпека стосується захисту життєво важливих інтересів людини (і більш глобально — суспільства, держави). Неправдива, неповна, невчасна інформація може нанести шкоду. Особливо вразливі у цьому контексті підлітки. Вони можуть не знати, яку інформацію можна викладати в мережу, а яку не варто. Інколи підлітки не можуть правильно зреагувати на матеріали з мережі з різних причин. Робота у цьому напрямку для викладачів та батьків дуже важлива. Безконтрольний доступ до інтернету може мати негативні наслідки для підлітка.

Очікувані відповіді:

1 Група: «Типи загроз»

Особиста безпека	Безпека інших	Розвиток персональної інформації
• загроза отримання недостовірної чи неправдивої інформації • формування залежності (ігрової, комп'ютерної,інтернет) • ознайомлення з порнографічними матеріалами, ненормативною лексикою,інформацією суїцидального характеру, расистського,ненависницького змісту. • спілкування з небезпечними людьми (збоченці,шахраї, грифери) • залучення до виконання противоправних дій (хакерство, порушення прав та свободінших)	• матеріали, існування та використання яких може стати причиною посягання на безпеку оточуючих (наприклад,інформація про створення вибухівки) • свідоме та несвідоме введення в оману інших • вчинення протиправних дій, що тягнуть за собою відповідальність згідно з чинним законодавством • кібербулінг - свідоме цькування та приниження перед усім однолітнів.	• розголошення персональної та конфіденційної інформації (прізвища, імена, контакти, секретні дані кредитних карток, номери телефонів) • загроза зараження ПК вірусами різної категорії • небезпека завантаження програм зі шкідливими функціями.

Слово викладача: Це найбільш поширені типи загроз, з якими може зіштовхнутися підліток в Інтернеті, викладаючи чи переглядаючи сумнівну інформацію. Від деяких з них можна захиститися технічними засобами, але більшість вимагають комплексного підходу. Наприклад, у розібратися у цьому допоможе безкоштовний онлайн-курс від порталу Prometheus — “Основи інформаційної безпеки”. Курс містить інформацію, яка буде цікава лише тим, хто захоплюється ІТ (історія появи вірусів). Але є й уроки, де розкриваються принципи захисту під час спілкування в соцмережах, при купівлі чогось в Інтернеті тощо.

2 група – Захист держави, щодо забезпечення інформаційної безпеки.

Для забезпечення захисту громадян кожна держава будує відповідну інформаційну політику щодо інформаційної безпеки.

В Україні політика гарантування інформаційної безпеки регламентується цілою низькою законодавчих актів, законів.

- ✓ Основним законодавчим актом в Україні, який регулює забезпечення захисту інформації, що належить особистості (громадянину), є Закон України « Про захист персональних даних».
- ✓ Конституція України, що стала гарантом побудови демократичної правової держави, не могла не врахувати загальносвітових тенденцій інформатизації суспільства. Тому ряд її статей (зокрема ст. 17, 32, 34) визначають забезпечення інформаційної безпеки, як одну з найважливіших функцій держави і мають стати основою розвитку інформаційного законодавства.
- ✓ Закон України "Про державну таємницю» січень 1994 року
- ✓ Концепція національної безпеки України
- ✓ Закони України "Про інформацію"
- ✓ Закон України "Про захист інформації в автоматизованих системах"

інші нормативно-правові акти, а також міжнародні договори України, що стосуються сфери інформаційних відносин

Всього, за нашими підрахунками, на сьогодні в Україні діє близько 60 нормативних актів, що стосуються регулювання відносин в інформаційній сфері. Крім того, видано низку відомчих актів Держкомсекретів України – циркулярних листів, роз'яснень, методик тощо (понад 15), які є обов'язковими для усіх державних органів, підприємств, установ, організацій під час здійснення ними функцій щодо забезпечення охорони інформації з обмеженим доступом, перш за все – державної таємниці.

3 група – Уникнення загроз під час роботи в Інтернеті.

- Небажано розміщувати персональну інформацію в Інтернеті. Персональна інформація – це ваше повне ім'я, прізвище, номер мобільного телефону, адреса електронної пошти, домашня адреса, фото з вами, членами вашої родини, друзями.
- Не відповідайте на спам (небажану електронну пошту).
- Дотримуйтесь етики спілкування.
- Не розсилайте листи з будь-якою інформацією незнайомим людям без їхнього прохання - це сприймається як "спам", і звичайно засмучує користувачів мережі.
- Використовуйте тільки ліцензійне програмне забезпечення. Установлюйте програми тільки з офіційних джерел. Перед установленням читайте відгуки інших користувачів, якщо вони доступні.
- Установлюйте та оновлюйте антивірусне програмне забезпечення як на стаціонарні, так і на мобільні комп'ютери.
- Завжди встановлюйте оновлення операційної системи та іншого программного забезпечення.
- Використовуйте надійні паролі.

- Приєднуйтеся тільки до перевірених Wi-Fi-мереж. Не відправляйте важливі дані через публічні та незахищеніWi-Fi-мережі.
- Установіть фільтр спливаючих вікон у браузері.
- Перевіряйте сертифікат безпеки сайтів у вигляді замка в адресному рядку браузера та URL-адреси веб-сайтів, щоб визначити, чи не підроблений сайт ви відвідуєте.
- Створюйте резервні копії важливих для вас даних, зберігайте їх на носіях даних, відключених від мережі Інтернет.

III. Первинне закріплення знань.

Установіть відповідність між терміном та його визначенням:

А. Конфіденційність	1. Дії кібер – зловмисників або шкідливої програми, спрямовані на захоплення, редагування чи видалення інформаційних даних віддаленої системи
Б. Цілісність	2. Стан, за якого потрібний інформаційний ресурс перебуває у вигляді, необхідному користувачеві, у місці, необхідному користувачеві, й у той час, коли він йому необхідний.
В. Доступність	3. Стан, за якого інформаційні дані не можуть бути отримані неавторизованим користувачем або процесом.
С. Хакерська атака	4.Захист точності та повноти інформаційних даних й програмного забезпечення.

Відповідь: А - 3, Б – 4, В – 2, С – 1.

IV. Підбиття підсумків уроку. Рефлексія.

Повідомлення та обґрунтування оцінок.

Обговорімо, що ж нового ви дізналися на уроці, чи зможете в реальному житті застосувати отриманні знання.

Метод «Ланцюжок». Пропоную розпочинати висловлювання з формули:

- Про що ви дізнались на уроці…
- Використовуючи матеріал уроку, я зможу…
- Чи сподобався вам цей урок…

«На дерево дивись, як родить, а на людину – як робить!»

(українська народна мудрість)

Я бажаю вам завжди працювати плідно, вірити в себе і завжди досягати поставленої мети. Це вам допоможе у подальшому дорослому житті.

V. Інформація - інструктаж домашнього завдання.

Створіть буклет або інформаційний бюлетень із правилами безпечної поведінки користувача в Інтернеті відповідно до обраної цільової аудиторії:

- ✓ студенти;
- ✓ працівники банківської сфери;
- ✓ будівники;
- ✓ викладачі.