***За програмою 2017 року,***

***яка затверджена наказом МОН України від 23.10.2017 № 1407***

***Модуль. Інформаційна безпека (17 год.)***

***10(11) клас***

***Інформатика***

***Календарно-тематичне планування***

***Орієнтовне календарно-тематичне планування вибіркових модулів за навчальною програмою вибірково-обов’язкового предмету інформатика для учнів 10-11 класів загальноосвітніх навчальних закладів (рівень стандарту)***

***Модуль. Інформаційна безпека (17 год.)***

[**Навчальна програма**](http://teach-inf.at.ua/load/kabinet_informatiki/navchalni_programi/navchalna_programa_vibirkovo_obov_jazkovogo_predmetu_dlja_uchniv_10_11_klasiv_informatika_riven_standartu_2018_rik/39-1-0-2090) з інформатики (**рівень стандарту**) для 10-11 класів загальноосвітніх шкіл, затверджена [Наказом Міністерства освіти і науки № 1407 від 23 жовтня 2017 року](http://teach-inf.at.ua/10_klas/10_klas_2018/nmo-1407.pdf)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ уро-ку** | **Дата**  **уроку** | **Тема уроку** | **Примітки** |
| Тема 1. Основи безпеки інформаційних технологій | | | |
|  |  | Правила поведінки і безпеки життєдіяльності (БЖ) в комп’ютерному класі.  Основні поняття в області безпеки інформаційних технологій. Місце і роль автоматизованих систем в управлінні бізнес-процесами. Основні причини загострення проблеми забезпечення безпеки інформаційних технологій. Інформація та інформаційні відносини. Суб'єкти інформаційних відносин, їх інтереси та безпека, шляхи нанесення їм шкоди. Безпека інформаційних технологій. |  |
|  |  | Інструктаж з БЖД. Загрози безпеці інформації в автоматизованих системах. Основні джерела і шляхи реалізації загроз безпеки та каналів проникнення і несанкціонованого доступу до відомостей та програмного коду:   комп'ютерні віруси та шкідливе програмне забезпечення (Malware);   інтернет-шахрайство;   спам-розсилки;   несанкціонований доступ до інформаційних ресурсів та інформаційно-телекомунікаційних систем;   бот-мережі (botnet);   DDoS-атаки (Distributed Denial of Service);   крадіжка коштів;   «крадіжка особистості» (Identity Theft) |  |
|  |  | Інструктаж з БЖД. Основні ненавмисні і навмисні штучні загрози. |  |
|  |  | Інструктаж з БЖД. Технічні засоби добування інформації.  Програмні засоби добування інформації. |  |
| Тема 2. Забезпечення безпеки інформаційних технологій | | | |
|  |  | Інструктаж з БЖД. Об'єкти захисту. Види заходів протидії загрозам безпеки. Переваги та недоліки різних видів заходів захисту. Основні принципи побудови системи безпеки інформації в автоматизованій системі. |  |
|  |  | Інструктаж з БЖД. Правові основи забезпечення безпеки інформаційних технологій. Закони України та інші нормативно- правові акти, що регламентують відносини суб'єктів в інформаційній сфері та захист інформації. Відповідальність за порушення у сфері захисту інформації та неправомірного використання автоматизованих систем. |  |
|  |  | Інструктаж з БЖД. Основні захисні механізми, які реалізуються в рамках різних заходів і засобів захисту. |  |
|  |  | Інструктаж з БЖД. Ідентифікація та аутентифікація користувачів.  Розмежування доступу зареєстрованих користувачів до ресурсів автоматизованих систем. Реєстрація та оперативне оповіщення про події безпеки. |  |
|  |  | Інструктаж з БЖД. Криптографічні методи захисту інформації.  Контроль цілісності програмних і інформаційних ресурсів. |  |
|  |  | Інструктаж з БЖД. Виявлення атак.  Захист периметра комп'ютерних мереж.  Керування механізмами захисту. |  |
|  |  | Інструктаж з БЖД. Міжнародні стандарти інформаційної безпеки. |  |
| Тема 3. Забезпечення безпеки комп'ютерних систем і мереж | | | |
|  |  | Інструктаж з БЖД. Проблеми забезпечення безпеки в комп'ютерних системах і мережах. Типова корпоративна мережа. Рівні інформаційної інфраструктури корпоративної мережі. Мережеві загрози, вразливості і атаки. Засоби захисту мереж. |  |
|  |  | Інструктаж з БЖД. Призначення, можливості, і основні захисні механізми міжмережевих екранів (брандмауерів). Переваги та недоліки брандмауерів. Основні захисні механізми: фільтрація пакетів, трансляція мережевих адрес, проміжна аутентифікація, відхилення скриптів, перевірка пошти, віртуальні приватні мережі, протидія атакам, націленим на порушення роботи мережевих служб, додаткові функції. Політика безпеки при доступі до мережі загального користування. |  |
|  |  | Інструктаж з БЖД. Системи аналізу вмісту поштового і веб-трафіку (електронна пошта і НТТР). Політики безпеки, сценарії і варіанти застосування і реагування. |  |
|  |  | Інструктаж з БЖД. Віртуальні приватні мережі (VPN). Загрози, пов'язані з використанням VPN. |  |
|  |  | Інструктаж з БЖД. Антивірусні засоби захисту. Загальні правила застосування антивірусних засобів в автоматизованих системах. Технології виявлення вірусів. Можливі варіанти розміщення антивірусних засобів. Антивірусний захист, як засіб нейтралізації загроз. |  |
|  |  | Інструктаж з БЖД. Виконання індивідуальних та колективних проектів. |  |