Відокремлений структурний підрозділ

«Херсонський політехнічний фаховий коледж

Державного університету «Одеська політехніка»»

|  |  |
| --- | --- |
|  | **ЗАТВЕРДЖУЮ:**  Заступника директора з НВР  \_\_\_\_\_\_\_\_\_\_\_\_ Куценко О. І.  \_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_ 2021р. |

**Виховний захід**

на тему**:**

**Кібербезпека та інформаційна безпека**

**РОЗГЛЯНУТО ТА СХВАЛЕНО**

ЦК класних керівників \_\_\_\_\_\_\_\_\_\_\_\_\_ протокол № 2 від 22 жовтня 2020 р.

Голова ЦК

\_\_\_\_\_\_Шкарбуль О.В.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(підпис, ініціали, прізвище)

Херсон

2021

**Розробник(и):** Бабикін С.А, класний керівник 481 групи, відділення комп’ютерної і програмної інженерії.

**І. Напрям виховної роботи:** громадянське, правове, превентивне виховання

**ІІ. Мета:** ознайомити з поняттям «кібербезпека», «види кібербезпеки», введення про важливість інформаційної безпеки в ХХІ столітті

**ІІІ. Форма проведення: бесіда.**

**ІV. Хід проведення:**

Вступне слово класного керівника.

**Ознайомлення з поняттям кібербезпеки, його видами та застосуванням.** Визначення понять "глобальне інформаційне середовище". Функціональність інформаційних структур США. Аналіз інформаційної доктрини України та основ зовнішньополітичної інформаційної політики

Обговорення «Яка небезпека загрожує користувачу в Інтернеті»

Обговорення «Як студенти можуть використовувати отриманні навички в IT-сфері»

Оформлення:

Відео 1 "Про етичний хакінг та кібербезпеку компанії"

Відео 2 "Як зберегти персональні дані від кібератаки? Як зберегти паролі?"

Відео 3 "Безпека в Інтернеті для підлітків"

Відео 4 "СБУ vs ФСБ (2/9) кібербезпека"

Обладнання:

Комп’ютер, проектор, екран.

**Хід проведення**

**Вступне слово класного керівника**

Доброго дня!

Сучасні війни ведуться в інформаційному просторі за допомогою специфічних інформаційних видів озброєння. Інформація може бути як у вигляді засобу захисту, так і нападу, і все буде залежати лише від того, чий ресурс та пропаганда будуть потужнішими.

За останні 5-7 років глобальний кіберпростір усе більшою мірою розглядається всіма державами світу як один із найважливіших безпекових пріоритетів, оскільки його функціонування стає визначальним чинником розвитку економіки, військового, соціального та інших секторів. Стає все очевиднішою і подальша мілітаризація кіберпростору, а зусилля окремих держав, що намагаються попередити цей процес, вочевидь, малоефективні та залишаться такими ще тривалий час. Можна з упевненістю говорити, що нині кіберпростір переживає час «неосередньовіччя» з усіма його атрибутами: відсутність чіткого міжнародного права, розбудова системи відносин «клієнт-патрон», формування своєрідних «феодальних угідь» в інформаційній сфері.

Сучасна людина занурена в інформаційнийпростір, адже живе серед телебачення,книг, журналів, та комп'ютерних ігор. Таким чином, інформація відіграє все більшу роль в життєвому циклі людини, пронизує всю його діяльність та формується інформаційний спосіб життя. За рахунок цього сучасний інформаційний простір - дуже суперечливе, але водночас надзвичайно різноманітне за характером представлених ідеологій, точок зору, підхід до тих чи інших явищ.

**Поняття «кібербезпека»**

Кібернетична безпека (кібер безпека) - стану захищеності кібер простору держави в цілому або окремих об'єктів його інфраструктури від ризику стороннього кібернетичного впливу, за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання й нейтралізація реальних і потенційних викликів, кібернетичних втручань і загроз особистим, корпоративним та/або національним інтересам, відсутність якої може відсутність якої може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони[1].

Основою боротьби з кібертероризмом в будь якій країні - це підрозділ інформаційно - військових сил, якщо так можна сказати, що спочатку має на меті проведення наступальних і оборонних операцій в глобальній Інтернет мережі (війна в Інтернеті з конкретними об'єктами - це можуть бути країни, приватні компанії, соціальні верстви населення, будь які особи) [Відео 1].

**Види «кіберзлочинців»**

На сьогоднішній день можна виділити декілька найбільш поширених схем, якими користуються інтернет-злочинці:

* махінації з картками та платіжними системами;**2**
* обман користувачів через створення фіктивних інтернет-магазинів;
* шляхом імітації реалізації товару (послуг) через інтернет-аукціони, віртуальні дошки оголошень;**4**
* телефонні та інші шахрайства з метою отримання персональних платіжних даних.

Чатують всі ці нехороші люди на нас всюди: в інтернет-магазинах, соцмережах, навіть – у мобільних іграх.

Наприклад, схеми телефонних обманів бувають такі:

а) шахраї телефонують людині та повідомляють, що його близька людина терміново потребує допомоги та схиляють до переказу коштів;  
 б) на інтернет-аукціонах шахраї дізнаються реквізити банківської картки особи, а далі телефонують під виглядом працівника банку та під різними приводами схиляють до розголошення даних картки, за допомогою яких можливо здійснювати інтернет-платежі (зокрема, cvv-коду). Потім зловмисники використовують платіжні системи для виведення коштів з картки потерпілого;

в) на популярних інтернет-аукціонах шахраї знаходять оголошення про продаж товару, телефонують продавцю під виглядом покупця та погоджуються придбати товар. Далі пропонують потерпілому підійти до банкомату та ввести певну комбінацію нібито для отримання коштів. Насправді, шахраї диктують жертві спочатку реквізити її рахунку, потім реквізити свого рахунку та суму переказу. Як наслідок, потерпілий переказує кошти зі свого рахунку [Відео 2].

У США підрозділ, що складає кістяк таких операцій - це Кіберкомандування США, також існує установа, що називається «Кібернетичне командування ВПС США», основним завданням котрого є протидія ДОС - атакам на військово - повітряні сили США Кіберкомаандування Сполуучених Штаатів Амеерики - частина Збройних сил США, підпорядковане об'єднаному Стратегічному командуванню США (знаходиться на базі ВПС США Оффутт, штат Небраска) [2].

Огляд історії і керівництва КК. Кіберкомандування було засновано 23 червня 2009 року у відповідності з наказом Міністра оборони США Роберта Гейтса[2 Командування офіційно введено в дію 21 травня 2010 на території військової бази Форт-Мід, (штат Меріленд). Заплановане досягнення повної оперативної готовності в жовтні 2010 року[3]. Першим керівником кіберкомандування призначено генерала Кейта Александера (Keith B. Alexander), який займав до цього пост голови Агенства Національної безпеки США.

Місія USCYBERCOM планує, координує, об'єднує, синхронізує і проводить дії для: керування функціонуванням і захистом спеціалізованих інформаційних мереж Міністерства оборони США; готується до, і за наказом, проводить повний спектр військових дій укіберпросторі згідно з наказом, щоб вирішити проблеми у всіх галузях, гарантуючи Американську/Союзницьку свободу дій в кіберпросторі і унеможливлює це ж саме нашим супротивникам.

Кібернетичне командування ВПС США. Кібернетичне командування ВПС США (англ. Air Force Cyber Command AFCYBER) - одне з головних командувань військово-повітряних сил США - тимчасовий орган управління військами у структурі ВПС США, створений у вересні 2007[4]. Базується на військово-повітряній базі Барксдейл[4]. Подібно до того, як авіаційні і космічні підрозділи призвані до ведення розвідувальних, оборонних і наступальних дій в повітряному навколоземному і космічному просторі, кіберпідрозділ відповідає за кіберпростір. За словами секретаря ВПС Майкла Уїнна (Michael Wynn), необхідність створення військового кіберпідрозділу викликана активізацією діяльності іноземних хакерів проти США [Відео 4].

Задача і функції підрозділу. Проведення захисних і наступальних операцій, повязаних з вторгненням в ІТ-системи потенційного супротивника; захист інформаційно-технічних систем америкаських військових, а також критично важливих вузлів американськогоІнтернету; вивчення апаратних закладок і вразливостей, які можуть бути віддалено використані для виведення з ладу військових систем, або зняття з них даних.

**Обговорення «Яка небезпека загрожує користувачу в Інтернеті»**

**Загроза для дорослих:**

Багато літні люди не розуміють, що цікавого в Інтернеті. Однак поступово наші бабусі і дідусі починають активно використовувати переваги Мережі. Саме Інтернет дозволяє їм спілкуватися з близькими та рідними, які в даний момент знаходяться в іншому місті чи навіть країні. Тут можна знайти практично всю необхідну інформацію. Та й до ігор старше покоління не може залишитися байдужим. Молоді люди переживає, що їх батьки, бабусі і дідусі можуть стати жертвою шахраїв, які працюють саме через Інтернет. Близько 52% опитаних висловили стурбованість цим питанням.

**Загроза для дітей:**

Небезпеки в Інтернеті для дітей дещо відрізняються від загроз для дорослих. Найпоширеніші категорії небажаних факторів для малюків вже давно визначили психологи, батьки, педагоги і медики. Одним з найбільш серйозних видів небезпеки в Мережі для підростаючого покоління є отримання небажаної інформації. Це може бути порнографія, насильство, наркотики, азартні ігри, заборонена ідеологія і безліч іншого. Дитяча психіка не може повною мірою прийняти отримані знання. Це може значно відбитися на мисленні, психічному розвитку [Відео 3].

**Обговорення «Як студенти можуть використовувати отриманні навички в IT-сфері»**

Для забезпечення дедалі зростаючих потреб ринку праці у фахівцях з кібербезпеки в університеті, на кафедрі інженерії програмного забезпечення та кібербезпеки 2018 році була ліцензована нова спеціальність.

Для підготовка таких фахівців університет, зокрема кафедра інженерії програмного забезпечення та кібербезпеки має необхідний аудиторний фонд, сучасну комп’ютерну техніку, матеріально-технічне, методичне забезпечення, висококваліфікований  професорсько-викладацький склад.

На випускників даного напряму підготовки чекають підприємства та організації України, у тому числі Департамент кіберполіції Національної поліції України, які зараз тісно співпрацюють з університетом і кафедрою  інженерії програмного забезпечення та кібербезпеки в рамках підписаних договорів та угод про співпрацю.

У процесі навчання студенти опановують технології побудови комп’ютерних систем та мереж, методи та засоби захисту інформації та комп’ютерних і інформаційних систем; підходи, засоби та технології адміністрування систем та мереж, вивчають мови програмування, технології розробки програмних продуктів, методи та технології криптографічних перетворень, інженерно-технічного і адміністративно-організаційного захисту інформації.

Використані джерела:

1. Бурячок, В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа]; за заг. ред. д-ра техн. наук, професора В. Б. Толубка.— К.: ДУТ, 2015. — 288 с.
2. Гайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. — К.:Видавнича група BHV, 2009. — 608 с.:іл.
3. Девянин П.Н. Модели безопасности компьютерных систем. Управление доступом и информационными потоками. Учебное пособие для вузов. — М.: Горячая линия-Телеком, 2011. — 320 с.: ил.
4. Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем. Учебное пособие. — СПб: Университет ИТМО, 2014. – 95с.

* Відео 1 – URL: <https://youtu.be/REfxKB4snCk>
* Відео 2 – URL: <https://youtu.be/eZuXSLxrkyM>
* Відео 3 – URL: <https://youtu.be/k5m-vI6sFZU>
* Відео 4 – URL: https://youtu.be/uYN9mlLkI\_w