УДК 004.056
ГАБОРЕЦЬ ОЛЬГА АНДРІЇВНА
доктор філософії, доцент, доцент кафедри ОРД та інформаційної безпеки, Донецький державний університет внутрішніх справ
ORCID: https://orcid.org/0000-0001-7791-6795
ГОРЕЛОВ ЮРІЙ ПЕТРОВИЧ
кандидат технічних наук, доцент, доцент кафедри кібербезпеки та DATA-технологій, Харківський національний університет внутрішніх справ,
ORCID https://orcid.org/0000-0002-0330-5008
КОБЗЕВ ІГОР ВОЛОДИМІРОВИЧ
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем і технологій, Харківський національний економічний університет,
ORCID http://orcid.org/0000-0002-7182-5814

МЕТОДИЧНІ АСПЕКТИ ВИКЛАДАННЯ КИБЕРГІГІЄНИ У РАМКАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

Забезпечення кібербезпеки та кібергігієни є важливою проблемою для всіх державних та громадських інституцій, включаючи ЗВО, та громадян у будь-яких умовах. Масштабна війна, розв'язана РФ в Україні, зробила її ще більш актуальною. Одним з шляхів забезпечення кібербезпеки держави є обізнаність громадян у питаннях кібергігієни. Ключовими моментами є:

1. Захист особистих даних: У період військового конфлікту може зростати ймовірність кібератак на цілі. Дотримання кібергігієни допомагає громадянам захистити свої особисті дані, такі як фінансова інформація, особисте листування та інші конфіденційні відомості.

2. Запобігання дезінформації: В умовах війни поширення дезінформації та фейкових новин може бути знаряддям в інформаційній війні. Дотримання кібергігієни допомагає громадянам фільтрувати інформацію, перевіряти її на достовірність та не піддаватися маніпуляціям.

3. Захист від кібершпигунства: Під час військових конфліктів можуть активізуватися кібершпигуни, які намагаються отримати доступ до чутливої

інформації через кібератаки та інші методи. Дотримання заходів кібербезпеки допомагає захистити громадян від таких спроб.

4. Забезпечення кібербезпеки сім'ї та близьких: Громадяни можуть застосовувати знання про кібергігієну, щоб захистити не лише себе, а й своїх близьких від кіберзагроз. Це включає навчання дітей безпечній поведінці в інтернеті, захист сімейних пристроїв та мереж від кібератак та інші заходи.

5. Підтримка суспільної стабільності: Дотримання кібергігієни допомагає запобігти паніку, хаосу та негативним наслідкам поширення хибної інформації в період військового конфлікту.

Таким чином, кібергігієна стає важливим інструментом захисту цивільних прав та безпеки в умовах військового конфлікту, допомагаючи громадянам захиститися від кібератак, запобігти дезінформації та забезпечити безпеку себе та своїх близьких. Це визначає важливість ознайомлення студентів з основними кіберзагрозами та методами протидії.

Нині багато ЗВО України, особливо у східних областях, перейшли на дистанційний режим роботи, використовуючи різні системи та методи дистанційного навчання (ДН). Тому важливою стає проблема оптимального використання системи ДН для викладання курсів з кібергігієни.

Викладання кібергігієни через дистанційне навчання може бути ефективним та зручним способом навчання студентів, оскільки поєднання синхронних та асинхронних методів навчання дозволяє у певної мірі знівелювати вплив таких негативних факторів, як відключення світла, відсутність стійкого інтернет-з’єднання та ін. До основних методів та засобів реалізації системи ДН можна віднести:

1. Онлайн курси та лекції: Створення спеціалізованих онлайн курсів або лекцій з кібергігієни, доступних для студентів через платформи ДН.

2. Інтерактивні вебінари та семінари: Проведення інтерактивних вебінарів та семінарів із залученням експертів з кібербезпеки. Це дозволить студентам ставити запитання, обговорювати актуальні проблеми та ділитися досвідом у реальному часі.

3. Онлайн навчальні матеріали та тестування: Надання доступу до онлайн навчальних матеріалів, таких як відеоуроки, статті, інфографіка та тести з кібергігієни. Це дозволить студентам вивчати матеріали у своєму власному темпі та перевіряти свої знання за допомогою тестування.

4. Колективні проекти та завдання: Організація колективних проектів та завдань, спрямованих на розвиток навичок кібербезпеки.

5. Форуми та онлайн обговорення: Створення онлайн форумів та груп для обговорення питань кібербезпеки. Це дозволить студентам обмінюватися думками, ставити запитання та ділитися своїм досвідом, що сприяє глибшому розумінню теми.

6. Навчання через ігри та симуляції: Використання ігор та симуляцій для навчання основ кібербезпеки. Це може бути у вигляді інтерактивних кібертренажерів, які дозволять студентам практикувати різні аспекти безпечної поведінки у віртуальному середовищі.

Використання комбінації цих методів допоможе створити ефективну та цікаву програму навчання з кібергігієни через дистанційне навчання.

Але в той же час використання систем ДН підвищує ризики кіберзагроз і робить актуальним реалізацію дієвого кіберзахисту. Це комплексний процес, що включає різні заходи та практики для захисту інформаційних ресурсів від кіберзагроз. ЗВО має розробити політику кібербезпеки, яка містила б інструкції та рекомендації щодо забезпечення безпеки інформаційних ресурсів. ЗВО повинен регулярно проводити навчання співробітників та студентів з кібербезпеки, оновлювати програмне забезпечення та виправляти вразливості, захищати мережу ЗВО, використовуючи міжмережові екрани та інші технології, реалізувати захист облікових записів та резервне копіювання даних. Необхідно також проводити регулярний аудит безпеки, виявляти потенційні вразливості у системах та мережах, ідентифікувати загрози та оцінювати ефективність заходів захисту. Реалізація цих заходів дозволить знизити ризики потенційних кіберзагроз та підвищити рівень кібербезпеки ЗВО при здійсненні освітнього процесу в умовах воєнного стану.