компетентностей: уміння вчитися і бути здатним до саморозвитку; вміння критично мислити; вміння сформулювати проблему, знаходити нові розв'язання, діяти в нестандартних ситуаціях; вміння використовувати здобуті знання для особистісної реалізації; вміння бути конкурентоздатним і мобільним в суспільстві.

Список використаних джерел:

1. Брежнєва-Єрмоленко О.В., Лола І.В. Креативне середовище – основа інноваційної активності фахівців. *Проблеми формування та розвитку інноваційної інфраструктури: європейський вектор – нові виклики та можливості*: тези доповідей III Міжнародної науково-практичної конференції (м. Львів, 14-16 травня 2015 року). Львів: Видавництво Львівської політехніки, 2015. С. 625–626.

2. Дімітрова-Бурлаєнко С.Д. Креативне освітнє середовище як чинник формування готовності студентів технічних університетів до виявлення креативної компетентності у професійній діяльності. *Вісник університету імені Альфреда Нобеля. Серія «Педагогіка і психологія». Педагогічні науки*. 2018. № 1 (15). С. 102–106.

Захар ЛАКОЦЕНІН
здобувач вищої освіти 4 курсу ОС «бакалавр»
спеціальності 125 «Кібербезпека»
Науковий керівник: ***Валентина СПІВАЧУК***
кандидат філологічних наук, доцент кафедри іноземних мов,
Хмельницький національний університет,
м. Хмельницький

ВАЖЛИВІСТЬ ВИВЧЕННЯ КІБЕРБЕЗПЕКИ СТУДЕНТАМИ ЗВО

Кібербезпека стає все більш важливою темою в сучасному світі. З розвитком цифрових технологій збільшився і потенціал для кібератак. Тому важливо обговорити необхідність вивчення кібербезпеки та заходи, яких

можуть вжити окремі особи та організації, щоб захистити себе від кіберзагроз.

Перш за все, важливо розуміти значення кібербезпеки. Кібератаки можуть призвести до крадіжки особистої та конфіденційної інформації, фінансових втрат і навіть до пошкодження критично важливої інфраструктури. Оскільки наша залежність від цифрових технологій зростає, потенційний вплив кібератак стає все більш значним. Тому дуже важливо, щоб окремі особи та організації вживали заходів для свого захисту.

Наукові напрацювання вчених і практиків засвідчують, що професійна підготовка фахівців у сфері кібербезпеки є одним із напрямів державної політики у сферах національної безпеки і оборони, без якого є неможливими захищене передавання інформації і відповідно – науково-технічний та соціально-економічний розвиток країни. На основі вивчення академічних праць з'ясовано, що в умовах інформаційних війн, замахів на цілісність і суверенітет української держави питання підготовки фахівців із кібербезпеки вміщають в себе проблеми педагогічного, системного і міждисциплінарного характеру. Як свідчать останні дослідження і публікації, проблеми професійного розвитку фахівців з кібербезпеки є малодослідженими. Так, І. Діордіца у своїх статтях досліджує питання стандартизації підготовки фахівців із кібербезпеки та здійснює аналіз стану підготовки фахівців у сфері кібернетичної безпеки станом на 2015–2016 роки [2]. С. Мельник у науковій роботі визначає концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки у вищих навчальних закладах [1]. На теперішній час підготовка висококваліфікованих кадрів залишається ключовим елементом повноцінної життєдіяльності держави. Цей процес характеризується поєднанням потреб суспільства з сучасними інформаційними технологіями із подальшим закріпленням на рівні нормативно-правових актів.

Одним з найважливіших заходів, які можна вжити для посилення кібербезпеки, є освіта. Фахівці з кібербезпеки, які здатні захистити мережеву інфраструктуру будь-якого підприємства, зараз користуються великим попитом. Ті, хто прагне на практиці застосовувати свої детективні здібності й набуті знання, зробить хорошу кар'єру в галузі кібербезпеки. Люди та організації повинні знати про різні типи кіберзагроз і способи, якими вони можуть себе захистити. Це включає розуміння того, як розпізнати спроби фішингу, використання надійних паролів та оновлення програмного забезпечення. Навчаючи себе та інших, особи та організації можуть зменшити свою вразливість до кібератак.

Іншим важливим аспектом кібербезпеки є використання захисного програмного забезпечення. Сюди входить антивірусне програмне забезпечення, брандмауери та системи виявлення вторгнень. Таке програмне забезпечення може виявляти та запобігати багатьом видам кібератак і є важливим компонентом будь-якої стратегії кібербезпеки. Однак важливо зазначити, що жодне програмне забезпечення не може забезпечити повний захист, і особи та організації повинні вживати додаткових заходів для забезпечення своєї кібербезпеки.

Одним з таких додаткових заходів є використання двофакторної автентифікації. Вона передбачає вимогу до користувачів надати дві форми ідентифікації перед тим, як отримати доступ до конфіденційної інформації або систем. Двофакторна автентифікація значно знижує ризик несанкціонованого доступу і широко використовується банками, медичними установами та іншими організаціями, які обробляють конфіденційні дані.

Шифрування - ще один важливий аспект кібербезпеки. Шифрування передбачає перетворення даних на код, який може прочитати лише той, хто має ключ для його розшифрування. Це може допомогти захистити конфіденційну інформацію від несанкціонованого доступу і зазвичай

використовується для електронної пошти, передачі файлів та онлайн-транзакцій.

На додаток до цих заходів, організаціям також важливо мати комплексну стратегію кібербезпеки. Вона повинна включати регулярні аудити безпеки, плани реагування на інциденти та програми навчання співробітників. Застосовуючи проактивний підхід до кібербезпеки, організації можуть мінімізувати ризик кібератак і бути краще підготовленими до реагування, якщо атака все ж таки відбудеться.

Ще одним ключовим елементом кібербезпеки є співпраця. Кібератаки можуть мати далекосяжні наслідки, тому організаціям важливо працювати разом, обмінюючись інформацією та ресурсами. Це включає обмін розвідданими про загрози, найкращими практиками та інструментами безпеки. Співпраця може допомогти покращити загальний рівень кібербезпеки та зменшити вплив кібератак.

Нарешті, важливо визнати, що кібербезпека – це безперервний процес. Кіберзагрози постійно розвиваються, і окремі особи та організації повинні відповідно адаптувати свої стратегії кібербезпеки. Залишаючись поінформованими та діючи на випередження, особи та організації можуть випередити кіберзагрози та захистити себе від потенційної шкоди.

Отже, кібербезпека є критично важливим питанням, яке впливає на людей та організації всіх типів. Застосовуючи проактивний підхід до кібербезпеки, навчаючи себе та інших, а також впроваджуючи комплексну стратегію кібербезпеки, особи та організації можуть зменшити свою вразливість до кіберзагроз і захистити себе від потенційної шкоди.

За останні роки кібератаки стали більш витонченими, а кіберзлочинці постійно знаходять нові способи використання вразливостей. До найпоширеніших типів кіберзагроз належать фішингові атаки, шкідливе програмне забезпечення, програмивимагачі та атаки на відмову в обслуговуванні.

Фішингові атаки передбачають надсилання шахрайських електронних листів або повідомлень, які виглядають як повідомлення з легітимного джерела, з метою обманом змусити людей надати конфіденційну інформацію, таку як облікові дані для входу в систему або дані кредитних карток. Шкідливе програмне забезпечення - це шкідливе програмне забезпечення, призначене для пошкодження, порушення роботи або отримання несанкціонованого доступу до комп'ютерної системи. Програми-вимагачі – це тип шкідливого програмного забезпечення, яке шифрує файли і вимагає оплату в обмін на ключ до розшифровки. Атаки на відмову в обслуговуванні полягають у перевантаженні сервера або мережі трафіком, внаслідок чого вони стають недоступними для законних користувачів.

Важливо зазначити, що кібератаки можуть мати серйозні наслідки не лише для окремих осіб та організацій, але й для суспільства в цілому. Наприклад, кібератака на об'єкти критичної інфраструктури, такі як електромережі або транспортні системи, може спричинити масштабні перебої в роботі і навіть поставити під загрозу життя людей.

Крім того, кібератаки загрожують не лише великим організаціям. Малий бізнес та приватні особи також є вразливими і можуть стати мішенню саме тому, що їх вважають легшою ціллю.

Тому важливо, щоб кожен серйозно ставився до кібербезпеки і вживав належних заходів для захисту від кіберзагроз. Це включає в себе впровадження захисного програмного забезпечення, використання надійних паролів, двофакторну автентифікацію та пильність щодо підозрілих електронних листів або повідомлень.

Крім того, важливо, щоб окремі особи та організації працювали разом над покращенням кібербезпеки. Це може включати обмін інформацією та передовим досвідом, а також повідомлення про кіберзагрози та інциденти відповідним органам влади.

Таким чином, кібербезпека є критично важливим питанням, яке стосується кожного. Розуміючи природу кіберзагроз і вживаючи належних заходів для свого захисту, окремі особи та організації можуть зменшити свою вразливість до кібератак і сприяти створенню більш безпечного та захищеного цифрового середовища. Сучасна безпекова ситуація як у державі, так і світі в цілому кардинально змінюється, що є поштовхом для появи якісно нових регуляторів, які у своєму арсеналі матимуть ефективні важелі впливу на суспільні і соціальні відносини в кібернетичній сфері. Ключовим завданням державної кібербезпекової політики дедалі виразніше виступає створення гарантованих умов реалізації національних інтересів у сфері освіти.

Список використаних джерел:

1. Мельник С. Концептуальні основи організації професійної підготовки майбутніх фахівців із кібербезпеки. *Педагогічні науки: теорія, історія, інноваційні технології*. 2016. № 10. С. 79–88. URL: http://nbuv.gov.ua/UJRN/pednauk_2016_10_9

2. Diorditsa I. State of training of cyber security specialist. Visegrad Journal on Human Rights, 2016. 6/1, 59–65.

Владислав МІХЄЄВ
здобувач вищої освіти 3 курсу ОС «бакалавр»
спеціальності 014 «Середня освіта. Фізична культура та спорт»
Науковий керівник: ***Марина НЕТРЕБА***
кандидат філологічних наук, доцент кафедри педагогіки та освіти,
Маріупольський державний університет,
м. Київ

ВИХОВАННЯ МОРАЛЬНО-ЦІННІСНИХ ОРІЄНТАЦІЙ УЧНІВ

Ціннісні орієнтації охоплюють усі сфери діяльності людини, сприяють осмисленню найбільш суттєвих сторін її способу життя,