вопросы. Контроль и самоконтроль обеспечивают обратную связь в учебном процессе - получение педагогом и учеником информации о степени трудности, типичные недостатки, что приводит к необходимости внесения в этот процесс соответствующих изменений и постоянного его совершенствования.

Для возможности самопроверки каждого ученика по той или иной теме, сайте в разделах «Тестовые задания» и «Вопросы для самоконтроля» можно опубликовать задания для самопроверки, а ученики дома, без вспомогательных материалов их смогут выполнить.

Ключевые слова: *сайт, биология, основная школа, компьютерные технологии, педагогический эксперимент, сеть Интернет, уровень знаний, типы уроков.*

Stepanyuk A. V., Mironets L. P. The methodology of using the website in the process of teaching biology in a primary school.

The article describes the methodology of using the training site in the process of teaching biology. The site structure and sections that need to be provided for effective work are described.

The purpose of this article is to describe the methodology for using the site for educational purposes in the study of biology in basic school.

The results of a pedagogical experiment, which was conducted on the basis of the Public Institution Sumy Gymnasium No. 1, are presented. It is established that the website can be used: in an introductory lesson, to activate the cognitive process and communicate new knowledge; in the lesson - the purpose of which is to expand and deepen the knowledge of students; at the generalizing lesson and the lesson of the final control and correction of knowledge.

Also, using the site is productive in the lesson that precedes the practical work. Given the workload requirements of students in terms of homework, you can develop lessons using the training site at the homework stage.

The site can store all theoretical information for the lessons so that the student can access it at any time. During each lesson, students receive and try to absorb a fairly large amount of information. A significant role in this case is played by students' self-control in the form of self-examination of the depth of assimilation of educational material, self-assessment of the correctness of solving biological problems and answers to questions. Control and self-control provide feedback in the educational process - the teacher and student receive information about the degree of difficulty, typical shortcomings, which leads to the need to make appropriate changes in this process and to constantly improve it.

To enable each student to self-test on a particular topic or site, in the sections "Test Tasks" and "Questions for Self-Control", you can publish tasks for self-testing, and students at home can complete them without supporting materials.

Key words: *site, biology, basic school, computer technology, pedagogical experiment, Internet, knowledge level, types of lessons.*

УДК 004.72.056.52:004.3]-057.177
DOI 10.5281/zenodo.3547760

Ю. М. Ткач
ORCID ID 0000-0002-8565-0525
Чернігівський національний
технологічний університет

ФОРМУВАННЯ ГОТОВНОСТІ ДО ЗАПОБІГАННЯ КІБЕРЗАГРОЗАМ У МАЙБУТНІХ МЕНЕДЖЕРІВ ОРГАНІЗАЦІЙ ЯК ЕЛЕМЕНТУ ІНФОРМАТИЧНОЇ КОМПЕТЕНТНОСТІ

У статті висвітлено питання формування готовності до запобігання кіберзагрозам у майбутніх менеджерів організацій як елементу інформатичної компетентності. Під «готовністю» студента до запобігання кіберзагрозам запропоновано розуміти

формування установки особистості для своєчасного реагування нею на наявні або потенційно можливі явища і чинники, що створюють небезпеку їм особисто чи життєво важливим національним інтересам України у кіберпросторі. Основним із основних шляхів формування готовність до запобігання кіберзагрозам в межах освітньої програми підготовки майбутніх менеджерів організацій визначено необхідність доповнення курсу інформатики питаннями, що висвітлюють проблеми кібербезпеки. Запропоновано критерії сформованості готовності студентів до запобігання кіберзагрозам, а саме, позитивна внутрішня мотивація студентів щодо виявлення можливих загроз та їх уникнення; оволодіння студентами сучасними техніками та технологіями захисту від несанкціонованого доступу та заволодіння конфіденційною інформацією; формування умінь і навичок студентів щодо адекватної поведінки у відповідних життєвих ситуаціях; формування у студентів навичок самостійно оцінювати можливість реалізації загроз у процесі користування сучасними інформаційно-комунікаційними технологіями. Зроблено висновок, що система вищої освіти повинна бути обов'язково включена у процес забезпечення кібербезпеки держави. У контексті підготовки майбутніх менеджерів організацій, має бути сформована готовність до запобігання кіберзагрозам як складової інформатичної компетентності. Тобто, у процесі набуття інформатичної компетентності під час навчання інформатики у студентів має бути сформована внутрішня позиція суб'єкта щодо необхідності захисту власних інтересів та інтересів держави від несанкціонованого доступу, порушення конфіденційності та цілісності, а також отримані навички (досвід) щодо безпосереднього запобігання кіберзагрозам. У ході дослідження використано теоретичні та емпіричні методи. Основні результати дослідження, його положення й висновки можуть бути використані під час розробки робочих програм з інформатики для підготовки фахівців різних спеціальностей, зокрема, майбутніх менеджерів організацій, а також під час перепідготовки фахівців у системі післядипломної освіти. Подальшого дослідження потребують питання формування готовності до запобігання кіберзагрозам у фахівців інших галузей.

Ключові слова: *формування готовності, кіберзагрози, інформатична компетентність, менеджери організацій, критерії сформованості, студенти, навчання інформатики, професійна сфера діяльності.*

Постановка проблеми. Сьогодні в умовах активного розвитку й впровадження сучасних інформаційних технологій, інфраструктура підприємств та держаних установ набуває неструктурованого характеру, що тягне за собою неконтрольоване зростання вразливостей та загроз інформаційній безпеці організації та держави в цілому. З часом кількість загроз та інтенсивність їх реалізації може набути неконтрольованого характеру, а отже значна частина організацій (різних джерел фінансування) залишається незахищеною перед сучасними викликами інформаційного простору. Таким чином, виникає необхідність у формуванні готовності до запобігання кіберзагроз фахівців всіх галузей діяльності, майбутніх менеджментів організацій зокрема.

Аналіз актуальних досліджень. Дослідження проблеми формування готовності студентів до різних видів діяльності здійснювався багатьма вченими у різноманітних напрямках. Так, О. Ковальов, С. Рубінштейн, Є. Кузьмін, В. Ядов, Д. Узнадзе, Г. Голубєва та ін. розглядали готовність до діяльності як певний *психологічний стан;* Д. Узнадзе пов'язував готовність із феноменом "*установки*", яка визначається як готовність до активності у певному напрямку, що виникає на основі взаємодії потреб та середовища і впливає на людину в даний момент; А. Прангішвілі стверджував, що готовність до певної форми реагування формується під впливом певних зовнішніх і внутрішніх умов та усвідомленого чи неусвідомленого сприйняття інформації; Д. Катц, Г. Оллпорт та ін. описували готовність до діяльності як стійкість до зовнішніх та внутрішніх впливів, яка тісно пов'язується із нейрофізіологічними механізмами регуляції та саморегуляції поведінки людини тощо.

Незважаючи на значний доробок науковців у дослідженні проблеми формування готовності студентів до тих чи тих аспектів діяльності, питання формування готовності до запобігання кіберзагрозам у майбутніх менеджерів організацій сьогодні є надзвичайно актуальним та залишається малодослідженим.

Мета статті. Визначити шляхи формування готовності та критерії сформованості готовності до запобігання кіберзагрозам у майбутніх менеджерів організацій.

Виклад основного матеріалу. У Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. №2163-VIII визначаються правові й організаційні основи забезпечення захисту життєво важливих інтересів людини та громадянина, суспільства та держави, національних інтересів України в кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Даним законом визначено тлумачення таких понять як кібератака, кіберзагроза, кібербезпека, кіберзлочин (комп'ютерний злочин), кіберпростір, кіберрозвідка, кібертероризм, кібершпигунство, критична інформаційна інфраструктура тощо.

Згідно із цим документом *кіберзагроза* - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів. У цілому *кібербезпека* – захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [3].

Одним з об'єктів кібербезпеки є суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища.

Таким чином, система вищої освіти, в частині *формування готовності* до запобігання кіберзагрозам у суспільстві, має відігравати провідну роль.

Науковці по-різному тлумачать поняття «готовність». Г. Бокарева, Н. Бугакова, А. Громцева, Е. Леванова, А. Маркова і ін. «готовність» вони розглядали і як психічний феномен особистості, і як соціальне явище, що визначає активність людини в реальних умовах його існування і функціювання. Вони зазначали, що для того, щоб ефективно керувати процесом учіння й розвитком розумових здібностей студентів у навчанні, необхідно враховувати внутрішні умови розвитку особистості та індивідуальну своєрідність кожного студента.

С. Рубінштейн представляв «готовність» як установку особистості, а під «установкою особистості» він розумів, зайняту нею позицію, яка знаходиться у в певному відношенні до поставлених цілей й задач та виражається у вибірковій мобілізованості і готовності до діяльності, що спрямована на їх реалізацію. Утворення установки припускає входження суб'єкта в ситуацію і прийняття їм завдань, які в ній виникають [5].

Л. Божович у своєму трактуванні «готовності» відзначав, що важливою є внутрішня позиція індивіда, в свою чергу під внутрішньою позицією він розумів єдину систему реально діючих мотивів по відношенню до навколишньої сфери, самосвідомость, а також відношення до себе в контексті оточуючого середовища [2].

Тобто, під «готовністю» студента до запобігання кіберзагрозам ми будемо розуміти *формування установки особистості для своєчасного реагування нею наявні або потенційно можливі явища і чинники, що створюють небезпеку їх особисто чи життєво важливим національним інтересам України у кіберпросторі*. Цей стан допоможе успішно виконувати поточні завдання як у навчанні так і у подальшій трудовій діяльності, правильно використовувати набуті знання, отриманий досвід і свідомо регулювати свою поведінку у випадку кіберзагроз.

У загальному вигляді «готовність» до певних дій, в тому числі запобігання кіберзагрозам, представляє собою сукупність психологічних феноменів, таких як

внутрішня позиція особистості та підготовленість до діяльності. Таким чином, у структурі готовності до діяльності можна виділити два основних компонента – *особистісний* (внутрішня позиція суб'єкта) і *операційний* (довільна саморегуляція діяльності, розумовий розвиток і досвід).

Сформувати готовність до запобігання кіберзагром в межах освітньої програми підготовки майбутніх менеджерів організацій можна під час набуття студентами інформативної компетентності, тобто під час навчання інформатики.

С.А. Раков до складу ІКТ-компетентності включає такі складові:

1) методологічну – усвідомлення комп'ютера як основи інтелектуального технологічного оточуючого середовища, усвідомлення можливостей та обмежень застосування засобів ІКТ для розв'язування соціально й індивідуально значущих задач сьогодні й у майбутньому;

2) дослідницьку – усвідомлення комп'ютера як універсального технічного засобу автоматизації дослідження; володіння засобами ІКТ та методами застосувань і наукових досліджень у різних галузях знань;

3) модельну – усвідомлення комп'ютера як універсального засобу інформаційного моделювання; опанування професійними пакетами комп'ютерного моделювання для різних освітніх галузей та навчальних предметів;

4) алгоритмічну – усвідомлення комп'ютера як універсального виконавця алгоритмів і як універсального засобу конструювання алгоритмів; володіння базовими поняттями теорії алгоритмів, володіння сучасними засобами конструювання алгоритмів;

5) технологічну – усвідомлення комп'ютера як універсального автоматизованого робочого місця (АРМ) для будь-якої професії; володіння сучасними засобами ІКТ для розв'язування практичних задач [4].

Н.В. Баловсяк вважає, що інформаційна компетентність майбутнього економіста незалежно від змісту виконуваної ним професійної діяльності повинна визначати здатності та знання фахівця стосовно роботи з інформацією та комп'ютерними технологіями. На думку Н.В. Баловсяк [1] інформаційна компетентність включає три компоненти:

– інформаційну (здатність ефективної роботи з інформацією у всіх формах її представлення);

– комп'ютерну або комп'ютерно-технологічну (що визначає уміння та навички щодо роботи з сучасними комп'ютерними засобами та програмним забезпеченням);

– процесуально-діяльнісну (яка визначає здатність застосовувати сучасні засоби інформаційних та комп'ютерних технологій до роботи з інформацією та розв'язання різноманітних задач);

– особистісними якостями (які виражають здатність спеціаліста до успішного здійснення професійної діяльності, зокрема, здатність до рефлексії, самоусвідомлення власної діяльності, комунікативні здібності, здатність до самоорганізації та організації інших людей, можливості швидкої мобілізації та зміни характеру виконуваної діяльності).

Характеризуючи сутнісні ознаки інформативної компетентності в сучасних умовах, слід зазначити, що вони постійно змінюються. На неї дуже впливають суспільні виклики, загрози, швидкий темп розвитку технологій тощо.

Отже, під інформатичною компетентністю майбутнього менеджера організацій будемо розуміти *сукупність знань, вмінь та якостей особистості, яка інтегрує знаннями теоретичного та навички практичного характеру з інформатики та ІКТ, необхідних для діяльності в сучасному інформаційному просторі та професійній галузі.*

Що стосується *формування готовності до запобігання кіберзагрозам як складової інформатичної компетентності*, то реалізація цього завдання має здійснюватись шляхом доповнення курсу інформатики питаннями, що висвітлюють проблему кібербезпеки.

Наприклад, однією з тематик має стати забезпечення захисту бездротових мереж. Wi-Fi – це протокол бездротової передачі даних, що допомагає з'єднати певну кількість комп'ютерів у мережу, або підключити їх до Інтернету, з малим радіусом дії, що використовує радіохвилі. Більшість сучасних портативних пристроїв (ноутбуки, КПК,

смартфони) вже мають вбудовані засоби для роботи в бездротових мережах. Якщо у пристрої немає вбудованих бездротових можливостей, то їх можна додатково придбати і встановити [9].

Технологія Wi-Fi стрімко набирає популярність.

Сьогодні майже кожна доросла людина час від часу користується даним засобом зв'язку та передачі даних.

У межах теми необхідно висвітлити питання:

1. Що таке Wi-Fi, коли він з'явився і чим він корисний?
2. Набір стандартів IEEE 802.11 b/g/n/ac.
3. Що ми розуміємо під небезпекою в комп'ютерних мережах?
4. Особливості загроз безпеки в бездротових мережах.
5. Чому не можна забороняти Wi-Fi?
6. Основні способи атак на безпровідні мережі.
7. Способи захисту.
8. Приклад злому соціальної мережі у відкритому Wi-Fi.
9. Поради: як зробити домашню мережу безпечнішою?
10. Поради: як безпечніше використовувати "Free Wi-Fi".

Особливу увагу при цьому варто звернути саме на аспекти небезпек, можливих загроз, способів атак, а також дати поради щодо убезпечення себе під час користування Wi-Fi, а саме для того, щоб зробити домашню мережу безпечнішою необхідно систематично змінювати пароль на роутері, відключати віддалене керування та трансляцію SSID, користуватись надійними стандартами захисту, вимкнути WPS(QSS), налаштувати firewall, користуватись та налаштовуйте антивірус. Якщо ж ви використовуєте "FREE Wi-Fi", то варто дотримуватись таких правил:

1. Вимкніть функцію автоматичного виявлення та підключення до доступних мереж.
2. Використовуйте безпечний протокол з'єднання HTTPS (наприклад, розширення для браузера – HTTPS Everywhere)
3. Вимкніть загальний доступ до файлів і папок.
4. Використовуйте **VPN** для підключення до доступу (HotSpot Shield, Spot Flux).
5. Використовуйте браузер **TOR.**
6. Відмовтеся від передачі конфіденційних або персональних даних за протоколами, незахищеним стійкими алгоритмами шифрування.
7. Не використовуйте інтернет-банкінг через публічні мережі Wi-Fi.

Разом з тим, обов'язковим питанням, на яке треба звернути увагу студентів це соціальна інженерія. *Соціальна інженерія,* з точки зору безпеки – злочинне вивідування даних [6].

Тобто, це сукупність методів, що спираються на психологічні особливості людей (цікавість, довіра, звичка тощо).

Це можуть бути прояви фітингу, як складової соціальної інженерії. Наприклад, створення підробленої сторінки сайту банку чи магазину тощо, з метою заволодіння конфіденційною інформацією користувача; або розсилання листів начебто від банків з проханням перейти за посиланням та авторизуватись тощо.

Варто дати поради майбутнім менеджерам організацій як уникати таких небезпек та загроз. Серед порад варто виділити наступні:

1. Бути пильним та уважним. Звертати увагу на деталі на сайтах, де авторизуєшся.
2. Якщо щось на сайті у вас викликає підозру перейдіть самостійно в браузері на офіційний сайт установи.
3. Критично ставтесь до електронних листів та подумайте перш ніж перейти за запропонованим посиланням.

Критеріями *сформованості готовності студентів до запобігання кіберзагрозам можна визначити наступні:*

– позитивна внутрішня мотивація студентів щодо виявлення можливих загроз та їх уникнення;

– оволодіння студентами сучасними техніками та технологіями захисту від несанкціонованого доступу та заволодіння конфіденційною інформацією;

– формування умінь і навичок студентів щодо адекватної поведінки у відповідних життєвих ситуаціях;

– формування у студентів навичок самостійно оцінювати можливість реалізації загроз у процесі користування сучасними інформаційно-комунікаційними технологіями.

Висновки та перспективи подальших наукових розвідок. Дослідження показало, що важливим завданням сьогодні є забезпечення інформаційної безпеки держави, кіберпростору зокрема. Сприяти цьому мають як державні так і недержавні установи. Система вищої освіти повинна бути обов'язково включена у процес виконання даного завдання. У контексті підготовки майбутніх менеджерів, має бути сформована готовність до запобігання кіберзагрозам як складової інформатичної компетентності.

Проведений аналіз поняття інформатичної компетентності дозволив зробити висновки: по-перше, інформаційна компетентність може розглядатися як інтегрована категорія, що включає сукупність знань, умінь і навичок виконання різних видів діяльності в галузі інформатики; по-друге, інформаційна компетентність майбутнього фахівця має бути безпосередньо пов'язана із професійною сферою діяльності; по-третє, інформаційна компетентність має забезпечувати формування установок особистості для своєчасного реагування нею на наявні або потенційно можливі явища і чинники, що створюють небезпеку їх особисто чи життєво важливим національним інтересам України у кіберпросторі.

Тобто, у процесі набуття інформатичної компетентності під час навчання інформатики у студентів має бути сформована внутрішня позиція суб'єкта щодо необхідності захисту власних інтересів та інтересів держави від несанкціонованого доступу, порушення конфіденційності та цілісності, а також отримані навички (досвід) щодо безпосереднього запобігання кіберзагрозам.

Подальшого дослідження потребують питання формування готовності до запобігання кіберзагрозам у фахівців інших галузей.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

1. Баловсяк, Н. (2004). Інформаційна компетентність фахівця. Педагогіка і психологія професійної освіти, 5, 21-28. (Balovsiak, N. (2004). Information competence of a specialist. Pedagogy and psychology of professional education, 5, 21-28).
2. Божович, Л. И. (1997). Проблемы формирования личности. Избранные психологические труды; под ред. Д. И. Фельдштейна. Москва – Воронеж. (Bozhovych, L. Y. (1997). Problems of personality formation. Selected psychological works; ed. D. I. Feldstein. Moskva – Voronezh).
3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 р. №2163-VIII (Law of Ukraine "On the Basic Principles of State Support for Gifted Children and Youth in Ukraine") (2017). Retrieved from: http://zakon.rada.gov.ua/laws/show/2163-19.
4. Раков, С.А. (2005). Сучасний учитель інформатики: кваліфікація і вимоги. Комп'ютер у школі та сім'ї, 3, 35-38. (Rakov, S.A. (2005). Modern Teacher of Informatics: Qualifications and Requirements. Computer at school and family, 3, 35-38).
5. Рубинштейн, С. Л. (2000). Основы общей психологии. Санкт-Петербург: Питер. (Rubinstein, S. L. (2000). Fundamentals of general psychology. Saint Petersburg: Piter).
6. Соціальна інженерія. Режим доступу: https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F. (Social engineering. Retrieved from: https://uk.wikipedia.org/wiki/%D0%A1%D0%BE%D1%86%D1%96%D0%B0%D0%BB%D1%8C%D0%BD%D0%B0_%D1%96%D0%BD%D0%B6%D0%B5%D0%BD%D0%B5%D1%80%D1%96%D1%8F).

7. Tkach Y. (2016). Mathematization of knowledge – the core of fundamentalization of proffeshinal training of the future economists. Science and Education a New Dimension. Pedagogy and Psychology, IV(40), Issue 81, 70-72.
8. Tkach Y. (2015). The issue of fundamentalization of professional training of future economists. Science Education Innovation. Association Scientific and Applied Research, Bulgaria, Volume 5, 54-58.
9. Wi Fi. Режим доступу: http://www.dut.edu.ua/uploads/l_1080_57518433.pdf (Wi Fi. Retrieved from: http://www.dut.edu.ua/uploads/l_1080_57518433.pdf).

Ткач Ю. Н. Формирование готовности к предупреждению киберугроз у будущих менеджеров организаций как элемента информатической компетентности.

В статье освещены вопросы формирования готовности к предотвращению киберугрозами в будущих менеджеров организаций как элемента информатической компетентности. Под «готовностью» студента к предотвращению киберугроз предложено понимать формирование установки личности для своевременного реагирования ней на имеющиеся или потенциально возможные явления и факторы, создающие опасность им лично или жизненно важным национальным интересам Украины в киберпространстве. Основным из путей формирования готовности к предотвращению киберугрозами в рамках образовательной программы подготовки будущих менеджеров организаций определена необходимость дополнения курса информатики вопросами, освещающих проблемы кибербезопасности. Предложены критерии сформированности готовности студентов к предотвращению киберугрозами. Сделан вывод, что система высшего образования должна быть обязательно включена в процесс обеспечения кибербезопасности государства. В контексте подготовки будущих менеджеров организаций, должна быть сформирована готовность к предотвращению киберугрозами как составляющей информатической компетентности. То есть, в процессе приобретения информатической компетентности при обучении информатики студентов должна быть сформирована внутренняя позиция субъекта о необходимости защиты собственных интересов и интересов государства от несанкционированного доступа, нарушение конфиденциальности и целостности, а также полученные навыки (опыт) по непосредственному предотвращения киберугрозами. В ходе исследования использованы теоретические и эмпирические методы. Основные результаты исследования, его положения и выводы могут быть использованы при разработке рабочих программ по информатике для подготовки специалистов различных специальностей, в частности, будущих менеджеров организаций, а также во время переподготовки специалистов в системе последипломного образования. Дальнейшего исследования требуют вопросы формирования готовности к предотвращению киберугрозами у специалистов других отраслей.

Ключевые слова: *формирование готовности, киберугрозы, информатическая компетентность, менеджеры организаций, критерии сформированности, студенты, обучение информатики, профессиональная сфера деятельности.*

Tkach Y. Formation of preparedness for the prevention of cyber threats in future managers of organizations as a element of informative competence.

The article covers the issue of preparedness for preventing cyber threats from future managers of organizations as an element of informational competence. Under the "readiness" of the student to prevent cyber threats, it is suggested to understand the formation of a person's setting for its timely response to existing or potentially possible phenomena and factors that jeopardize them personally or vital national interests of Ukraine in cyberspace. One of the main ways of forming readiness to prevent cyber threats within the education program of future managers of organizations is the need to supplement the course on informatics issues that cover the problems of cybersecurity. The criteria for the formation of students' readiness for preventing cyber threats, namely, positive internal motivation of students in identifying possible threats and

avoiding them, are suggested. Mastering students with modern techniques and technologies of protection against unauthorized access and confiscation of confidential information; the formation of students' skills and abilities in relation to adequate behavior in relevant life situations; the formation of students' skills to independently assess the possibility of implementing threats in the process of using modern information and communication technologies. It is concluded that the system of higher education must be included in the process of ensuring the cyber security of the state. In the context of the training of future managers of organizations, there should be preparedness to prevent cyber threats as a component of informational competence. That is, in the process of acquiring informational competence during the study of computer science students should form the internal position of the subject regarding the need to protect their own interests and interests of the state from unauthorized access, violation of confidentiality and integrity, as well as skills acquired (experience) regarding the direct prevention of cyber threats. During the research, theoretical and empirical methods were used. The main results of the study, its position and conclusions can be used in the development of working programs in computer science for the training of specialists in various specialties, in particular, future managers of organizations, as well as during retraining of specialists in the system of postgraduate education. Further research needs the issue of preparedness to prevent cyber threats from other industry professionals.

Key words: *readiness formation, cyber threats, computer competence, managers of organizations, criteria of formation, students, computer science training, professional field of activity.*