Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.

Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.

ISSN 2413-158X (online)
ISSN 2413-1571 (print)

http://fmo-journal.fizmatsspu.sumy.ua/

Олексюк В.П. Формування у майбутніх учителів інформатики компетентностей безпечної діяльності у комп'ютерних мережах // Фізико-математична освіта : науковий журнал. – 2017. – Випуск 4(14). – С. 244-249.

Oleksiuk Vasyl. Development Of Future Computer Science Teachers' Competence Of The Safe Activity In The Computer Networks // Physical and Mathematical Education : scientific journal. – 2017. – Issue 4(14). – P. 244-249.

УДК 378.126:004.056

В.П. Олексюк
Тернопільський національний педагогічний університет імені Володимира Гнатюка, Україна
oleksyuk@fizmat.tnpu.edu.ua

ФОРМУВАННЯ У МАЙБУТНІХ УЧИТЕЛІВ ІНФОРМАТИКИ КОМПЕТЕНТНОСТЕЙ БЕЗПЕЧНОЇ ДІЯЛЬНОСТІ У КОМП'ЮТЕРНИХ МЕРЕЖАХ

Анотація. *У статті досліджено поняття кібернетичної та інформаційної безпеки. Автором визначено науково-методичні засади формування у майбутніх учителів інформатики фахових компетентностей у галузі інформаційної безпеки – неперервність та поетапність. На першому із визначених етапів запропоновано здійснювати формування у студентів компетентностей безпечної діяльності у освітньо-інформаційному середовищі ВНЗ. Завдання другого етапу полягають у вивченні студентами теоретичних основ інформаційної безпеки та формування навичок застосування засобів захисту комп'ютерних мереж. Їх розв'язання можливе у межах нормативних дисциплін циклу фахової підготовки майбутніх учителів інформатики. Третій етап підготовки запропоновано здійснювати у формі дослідження студентами їх власних інформаційних систем на предмет виявлення вразливостей та виявлення несанкціонованого проникнення до них. У дослідженні розглянуто такі основні компоненти професійних компетентностей вчителя інформатики: мотиваційно-ціннісний, організаційно-змістовний, когнітивно-операційний та особистісно-рефлексивний.*

Ключові слова: *кібербезпека, інформаційна безпека, майбутній учитель інформатики, компетентність, комп'ютерні мережі.*

Постановка проблеми. Впродовж останніх десятиліть розвиток мережних технологій забезпечив значні можливості щодо створення та використання інформаційних ресурсів. Поряд з цим наслідком стрімкого розвитку глобальних комп'ютерних мереж є виникнення негативних явищ, пов'язаних з інформаційною безпекою, зокрема, втручання у приватне життя людини, знищення особистих або корпоративних даних. У зв'язку з цим виникла потреба у підготовці фахівців у галузі кібернетичної та інформаційної безпеки. Системне вирішення проблеми можливе лише за умови розвитку компетентностей безпечної діяльності в комп'ютерних мережах та Інтернеті. Зазначений процес повинен бути неперервним та здійснюватися упродовж усього життя, починаючи із загальноосвітньої школи. У цьому контексті важливою проблемою є навчання вчителів інформатики основам інформаційної безпеки. На нашу думку, у педагогічних ВНЗ зазначеній проблемі приділяється недостатня увага.

Аналіз актуальних досліджень. Затребуваність фахівців у галузі кібербезпеки підтверджено на законодавчому рівні, зокрема у нещодавно прийнятому законі "Про основні засади забезпечення кібербезпеки України". Відповідно вітчизняна вища школа здійснює підготовку фахівців у галузі захисту інформаційних технологій. У 2016 році затверджено стандарт спеціальності "125. Кібербезпека", у якому визначено загальні та спеціальні компетентності бакалаврів з кібербезпеки. У публікації О.В. Коржової досліджується проблема фундаментальності навчання та міжпредметних зв'язків у процесі підготовки майбутніх фахівців із організації інформаційної безпеки [6]. С.О. Воскобойніков виділяє компоненти професійної готовності фахівців з кібербезпеки: ноосферно-аксіологічний, інноваційно-формуючий, інформаційно-технологічний, проектно-технічний та моніторингово-оцінний [4].

Методологічною основою проблем інформаційної безпеки є філософія розвитку інформаційного суспільства та інформатизації освіти. Невід'ємними складниками цих процесів є підготовка компетентних фахівців [11]. Проблеми інформаційної безпеки є особливо актуальними у процесі становлення та розвитку відкритої освіти. В. Ю. Биков, досліджуючи проблематику навчального середовища відкритої освіти, серед вимог до його складу і структури виділяє вимоги щодо захисту засобів, технологій та інформаційних ресурсів від несанкціонованого доступу" [3, с. 52]. Розробленню методики забезпечення інформаційної безпеки у комп'ютерно орієнтованому навчальному середовищі присвячені дослідження О. М. Спіріна та В. Н. Ковальчук [12]. Проблеми оцінювання компетентностей педагогів та учнів досліджуються у публікаціях В. Ю. Бикова, О. В. Овчарук, О. М. Спіріна та інших [10]. О. Ю. Буров серед негативних чинників та ризиків діяльності у цифровому навчальному середовищі виділяє: відкритість учня для зовнішнього впливу, відсутність "живого" спілкування, фізіологічні ризики (вади постави, гіподинамія тощо), вади психічного розвитку (тривожність, мережна адикція), неконтрольований характер кіберзагроз, відсутність або несистемний характер застосування засобів захисту [1].

Мета статті. Визначити засадничі підходи розвитку компетентностей з інформаційної безпеки у майбутніх учителів інформатики, розробити окремі складники відповідної методичної системи.

Як показує досвід загальноосвітньої школи, провідним її фахівцем у галузі ІКТ є учитель інформатики [7]. У контексті забезпечення інформаційної безпеки він повинен бути здатним збалансовувати переваги та недоліки застосування мережних технологій у навчальному процесі. Під кібербезпекою розуміють стан захищеності комп'ютерних мереж. Відповідно завдання кібербезпеки полягають у захисті даних, що передаються в мережних системах, а завдання інформаційної безпеки пов'язані з діяльністю користувача. Вони полягають в захисті інформації, не залежно від носія, на якому зберігаються відповідні дані. Оскільки проблеми інформаційної та кібербезпеки знаходяться на межі педагогіки та ІКТ, то можна припустити, що висококваліфікований учитель інформатики буде спроможним здійснювати навчально-методичну діяльність з учнями та педагогами, а також забезпечити технічно-експертний супровід інформаційно-освітнього середовища школи.

У проекті стандарту підготовки бакалаврів зі спеціальності "0.14.09. Середня освіта (Інформатика)" серед предметних (спеціальних фахових) компетеностей фахівця визначено здатність формувати уміння безпечної діяльності школярів у комп'ютерній мережі та здатність впроваджувати засоби і методи захисту інформації та безпеки в мережі Інтернет. Проте, як показує досвід, розвиток відповідних компетентностей, зазвичай, не передбачений у навчальних планах педагогічних ВНЗ. Аналіз науково-педагогічних праць дослідників компетентнісного підходу дозволив виділити основні компоненти професійних компетентностей вчителя інформатики: мотиваційно-ціннісний, організаційно-змістовний, когнітивно-операційний та особистісно-рефлексивний [2]. На нашу думку, розвиток компетеностей з інформаційної безпеки повинен здійснюватися неперервно, проте здійснюватися поетапно упродовж усього терміну підготовки студента. На кожному із етапів навчання передбачаємо підготовку студентів, яка передбачає різнорівневе усвідомлення та протидію інформаційним та кіберзагрозам.

1. Етап розвитку компетентностей у процесі використання ІКТ як засобів організації діяльності.
2. Етап вивчення та застосування засобів захисту комп'ютерних мереж.
3. Етап дослідження студентами рівня кібербезпеки власних інформаційних систем.

На першому етапі доречно здійснювати формування у студентів компетентностей безпечної діяльності у освітньо-інформаційному середовищі ВНЗ. Нині важливою безпековою проблемою є створення єдиних систем автентифікації, які широко впроваджуються у сучасних університетах. Інтеграція у них хмарних та традиційних сервісів забезпечує легкий та уніфікований доступ викладачів та студентів до їх особистих даних, зокрема й через мережу Інтернет. Зазвичай, для автентифікації користувачів середовища використовують традиційний засіб – введення логіна та пароля. У інформаційно-освітньому середовищі навчальних закладів використовують єдину автентифікацію – доступ до різних (усіх) сервісів здійснюється за допомогою одного й того ж логіна й пароля. Такими сервісами можуть бути сайти, система електронного навчання, електронна пошта, віртуальна приватна мережа, бездротові мережі Wi-Fi тощо. Фахівці з безпеки, викладачі інформатики, а також студенти мають розуміти, що такий підхід несе суттєві загрози, особливо у випадку використання відкритих протоколів передавання даних.

У студентів варто формувати як складову їх інформаційної культури розуміння, що за цілісність власних даних першочергово несе відповідальність користувач-власник. З метою підвищення безпеки збереження даних викладачі та студенти, як користувачі інформаційно-освітнього середовища ВНЗ, повинні використовувати паролі достатньої складності та періодично змінювати їх. Ще однією тенденцією розвитку інформаційно-освітніх середовищ ВНЗ є використання персональних пристроїв у навчальному процесі. Крім доступу до власних бездротових мереж університети надають віддалений доступ викладачам та студентам до власної корпоративної мережі за допомогою технологій віртуальних приватних мереж. Зниження зазначених ризиків вбачаємо через підвищення рівня безпеки інформаційно-освітнього середовища через сегментацію комп'ютерних мереж та фільтрування трафіку, який передається у них, а також завдяки розвитку

в учасників освітнього процесу ІК-компетентностей щодо забезпечення належного рівня захищеності їх власних пристроїв.

Вивчення засобів захисту комп'ютерних систем (другий етап) має передбачати відповідну теоретичну та прикладну підготовку майбутнього вчителя інформатики. Розвиток відповідних компенетностей має здійснюватися упродовж вивчення практично усіх дисциплін професійної підготовки. Безпосереднє навчання основам інформаційної безпеки можливе у процесі вивчення окремих «класичних» курсів ("операційні системи", "теорія інформації і кодування", "комп'ютерні мережі та Інтернет", "програмування", "методика навчання інформатики"), а також комп'ютерної, виробничої, педагогічної та науково-педагогічної практик, у процесі написання курсових та кваліфікаційних робіт.

Важливими поняттями дисципліни "операційні системи" у контексті кібербезпеки вважаємо поняття процесу, файла, сеансу роботи користувача. На їх основі можна формувати компетентності щодо захисту операційних систем від вірусів. Теоретичні положення про типи вірусів та способи захисту від них доцільно підкріплювати практичними завданнями. Вивчення та знешкодження вірусних загроз можна здійснювати, організувавши віртуальні лабораторії у академічній хмарі університету [8].

У курсі "Комп'ютерні мережі" студенти вивчають теоретичні основи передавання даних. Фундаментальними поняттям, яке стосуються кібербезпеки є модель відкритих систем OSI. На її основі у студентів варто формувати розуміння принципів передавання даних у локальних мережах та Інтернеті. Належне засвоєння основ функціонування стеку протоколів TCP/IP є основою для розвитку навичок щодо фільтрування даних у складених мережах. Зазначені питання доречно вивчати на основі кількох ОС та програм-брандмауерів. При цьому незмінними залишаються принципи фільтрування та критерії, на основі яких приймається рішення про подальшу обробку пакета даних. Слід підкреслити важливу роль моніторингу процесів передавання трафіку. У зв'язку з цим у курсі можна передбачити виконання лабораторних робіт, які стосуються вивчення відповідних протоколів (SNMP).

Чимало питань, які стосуються захисту інформаційних систем, можуть вивчатися у курсі "Адміністрування комп'ютерних мереж". Базовими поняттями курсу, які стосуються кібербезпеки, вважаємо: обліковий запис користувача, автентифікація, авторизація, робоча група, домен, сервер, клієнт. Розглядаючи терміни, пов'язані з перевіркою достовірності облікових записів, варто зупинитися на сучасних підходах забезпечення автентифікації й авторизації (біометрична, двофакторана). У процесі адміністрування мережних сервісів ОС студентам пропонують узагальнену орієнтувальну основу діяльності, яка передбачає аналіз журналів ОС, у яких здійснюється фіксування подій, які стосуються функціонування системних сервісів, аудиту діяльності користувачів, встановлення програмного забезпечення. Робота журналами подій в ОС є важливою складовою ІК-компетентності фахівця у контексті здійснення ним моніторингу та протидії кіберзагрозам.

Підходи то централізованого адміністрування комп'ютерних систем можна ілюструвати на прикладі доменних мережних структур. Поряд із значними перевагами доменна модель забезпечення доступу до мережних ресурсів несе суттєві безпекові недоліки. Незважаючи на те, що деякі протоколи автентифікації у домені використовують ключі шифрування та передбачають обов'язкове підтвердження достовірності користувача третьою стороною, саме вдала кібератака на контролери домену може призвести до виведення з ладу усіх комп'ютерів мережі. Централізована модель адміністрування доменів може бути детально продемонстрована на прикладі доменних служб Active Directory. Як відомо усі об'єкти доменів містяться у ієрархічній базі даних – LDAP-каталозі. До його структурних одиниць – контейнерів можуть бути застосовані політики безпеки. Безпекові аспекти повинні бути присутні й у процесі вивчення Інтернет-сервісів (веб-, поштові, ftp-сервери). Крім моніторингу та статистики їх функціонування студентам можна запропонувати виконати конфігурування їх додаткових модулів, які, наприклад, забезпечують захист від спаму та вірусних атак. Цікавим підходом до вивчення курсу "Адміністрування комп'ютерних мереж" є використання проектних методик. Виконуючи навчальний проект, студенти налаштовують власні сервери. В учасників проектів слід формувати переконання та уміння здійснювати резервне копіювання власних ОС.

Значну роль у розвитку компетентностей з інформаційної безпеки належить курсу "Методика навчання інформатики". У зазначеному курсі доречно приділяти увагу підготовці студентів до критичного оцінювання ресурсів Інтернету. Відповідні навички дають змогу учителю інформатики уникати чималої кількості інформаційних загроз, а також формувати навички безпечної інформаційної діяльності в учнів. Важливими складовими ІК-компетентності вважаємо усвідомлення студентами фактів про те, що опубліковані в Інтернеті відомості про особу будуть доступними для усіх незалежно від бажання їх власника, а видалити відповідні дані буде практично неможливо. Студентам варто пояснювати та демонструвати на прикладах феномен "цифрової тіні" користувача, яка створюється внаслідок інформаційно-пошукової діяльності в Інтернеті. Вона формується без участі власника інформації і накопичується щоразу, коли відбувається пошук відомостей про користувача, у процесі електронного поштового розсилання, при індексації пошуковими системами сторінок з інформацією про особу.

Дослідження студентами захищеності власних інформаційних систем (третій етап підготовки) можливе у варіативній частині циклу професійної підготовки – у формі спецкурсів. Пропонуємо у них

здійснювати поглиблене вивчення питань кібербезпеки з використанням так званих задач на проникнення. Їх суть полягає у моделюванні способів випробування засобів захисту інформаційної системи. У процесі тестування на проникнення студент виконує роль зловмисника, який намагається порушити інформаційну безпеку мережі замовника. Виконання зазначених тестів дає змогу оцінити рівень захищеності мережі або веб-ресурсу та виявити вразливості, які можуть бути використані зловмисником. Перевагами задач на проникнення є: значна достовірність виявлених вразливостей, наочність отриманих результатів, практичний характер навчання. Недоліками зазначеної методики можна вважати: не можливість дослідження студентом дій більш компетентного зловмисника, недостовірність результатів, які свідчать про відсутність загроз, низький ступінь автоматизації [5].

Виконання задач на проникнення доцільно здійснювати у віртуальних хмарних лабораторіях [9]. Зокрема нами на основі платформи Apache CloudStack були розгорнуті кілька таких лабораторій. У них реалізовано такі можливості навчання основам інформаційної безпеки:

- функціонування значної кількості віртуальних машин (ВМ), які працюють під управлінням різних ОС;
- об'єднання та переміщення студентських ВМ у межах віртуальних мереж;
- робота з ВМ як через стандартні протоколи віддаленого доступу, так і через веб-інтерфейс;
- безпечне тестування вірусних загроз у хмарній інфраструктурі.

Недоліками реалізованих хмарних лабораторії можна вважати: значну трудозатратність створення шаблонів ВМ, неможливість використання деяких ОС, необхідність постійного супроводу хмари кваліфікованим фахівцем. Перед початком тестування студентам надають схему та опис IT-інфраструктури. У подальшому вони виконують дослідження вразливостей, пов'язаних з роботою мережних сервісів, криптографічних механізмів, помилками конфігурації, а також з людським фактором.

Студентам можна запропонувати виконання таких типів задач на проникнення.

1. Перехоплення даних автентифікації, які передаються через незахищені протоколи.
2. Одержання даних про ОС Linux сервера терміналів, на основі відомих даних автентифікації
3. Дослідження на вразливість веб-сайту, який розміщено на ВМ, копіювання його бази даних.
4. Дослідження журналу подій сервера, з метою виявлення підбору пароля користувача.
5. Пошук та моніторинг відкритого мережного порта Інтернет-сервера.
6. Отримання та розшифрування бази даних користувачів поштового сервера.
7. Пошук користувача ОС Windows, що видалив файл із спільного мережного ресурсу.

Висновки. Науково-методичні засади формування у майбутніх учителів інформатики фахових компетентностей у галузі інформаційної безпеки полягають у забезпеченні неперевності та поетапності процесу їх підготовки. Важливим є розвиток у студентів мотиваційно-ціннісного, організаційно-змістового, когнітивно-операційного та особистісно-рефлексивного складників фахових компетентностей. Розвитку мотиваційно-ціннісного та особистісно-рефлексивного компонентів можливий завдяки формуванню поглядів, переконань на інформаційну безпеку. Організаційно-змістовий та когнітивно-операційний складники можна розвивати у процесі вивчення теоретичних основ кібербезпеки. Формування умінь та навичок захисту інформаційних систем варто здійснювати опосередковано – у межах нормативних дисциплін, а також безпосередньо –у межах спецкурсів.

Список використаних джерел

1. Burov O. Y. Educational networking: human view to cyber defense [Електронний ресурс] / O. Y. Burov // Інформаційні технології і засоби навчання. – 2016. – Т. 52, вип. 2. – С. 144-156. – Режим доступу: http://nbuv.gov.ua/UJRN/ITZN_2016_52_2_15
2. Балик Н.Р. Формування інформаційних та соціальних компетентностей студентів з метою їх професійної підготовки у педагогічному університеті / Н.Р. Балик, Г.П. Шмигер // Науковий огляд. – 2016. – №1(22) – С. 14-21
3. Биков В. Ю. Навчальне середовище сучасних педагогічних систем / В. Ю. Биков // Професійна освіта: педагогіка і психологія / В. Ю. Биков. – Ченстохов: Вища Педагогічна Школа у Честохові, 2004. – С. 59–80.
4. Воскобойніков С. О. Професійна готовність до захисту інформації з обмеженим доступом спеціалістів інформаційної безпеки як науково-практична проблема в умовах глобалізації інформаційного простору /С. О. Воскобойніков // Науковий часопис Національного педагогічного університету імені М.П.Драгоманова. Серія 16. Творча особистість учителя: проблеми теорії і практики: збірник наукових праць. – № 25 (35). – К.: НПУ імені М.П.Драгоманова, 2015. – С. 7-11.
5. Кадан А. М. Виртуальные облачные лаборатории для задач тестирования на проникновение [Електронний ресурс]. – Режим доступу: http://ceur-ws.org/Vol-1761/paper24.pdf
6. Коржова О. В. Теоретичні аспекти міжпредметних зв’язків математичних дисциплін з дисциплінами циклу професійної підготовки майбутніх фахівців із організації інформаційної безпеки [Електронний ресурс] / О. В. Коржова – Режим доступу до ресурсу: http://fmo-journal.fizmatsspu.sumy.ua/publ/4-1-0-178.

7. Морзе Н.В. Підготовка педагогічних кадрів до використання комп'ютерних телекомунікацій Н.В. Морзе // Науковий часопис НПУ імені М. П. Драгоманова. Серія 2: Комп'ютерно-орієнтовані системи навчання. – № 6. – 2003. – С.12-25.
8. Олексюк В. П. Застосування віртуальних хмарних лабораторій у процесі підготовки майбутніх учителів інформатики / В. П. Олексюк // Науковий часопис НПУ імені М. П. Драгоманова. Серія 2: Комп'ютерно-орієнтовані системи навчання. – 2015. – №. 15. – С. 76-81.
9. Олексюк В. П. Проектування моделі хмарної інфраструктури ВНЗ на основі платформи Apache CloudStack. [Електронний ресурс] / В. П. Олексюк // Інформаційні технології і засоби навчання. – 2016. – №4. – Режим доступу до журн.: http://journal.iitta.gov.ua/index.php/itlt/article/view/1453/1074
10. Оцінювання інформаційно-комунікаційної компетентності учнів та педагогів в умовах євроінтеграційних процесів в освіті / Биков В. Ю., Овчарук О. В. та ін.– К. : Педагогічна думка, 2017. – 160 с.
11. Рамський Ю.С. Професійна діяльність вчителя в епоху інформатизації освіти [Електронний ресурс] / Ю.С. Рамський. – Режим доступу до ресурсу: http://enpuir.npu.edu.ua/handle/123456789/9387.
12. Спірін О. М. Методика забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи / О. М. Спірін, В. Н. Ковальчук // Інформаційні технології і засоби навчання, №1(21). – 2011.

References

1. Burov O. Y. Educational networking: human view to cyber defense [Electronic Resource] / O. Y. Burov // Information technologies and learning tools. – 2016. – V. 2(52). – P. 144-156. – Available from: http://nbuv.gov.ua/UJRN/ITZN_2016_52_2_15
2. Balyk N.R. Formation of informational and social competencies of students for professional training in pedagogical university / N.R. Balyk, H.P. Shmyher // Naukovyy ohlyad. – 2016. – №1(22) – P. 87-94
3. Bykov V.Yu. Educational environment of modern pedagogical systems / V.Yu. Bykov // Vocational education: pedagogy and psychology. – Czestochov: Higher Pedagogical School in Czestochov, 2004. – P. 59–80.
4. Voskoboinikov S. O. The factors and conditions of the development of information culture of teacher in a secondary education institution /S. O. Voskoboinikov // Scientific journal of NPU named after M. P. Drahomanov. Series 16. Creative personality of the teacher: problems of theory and practice. – № 25 (35). – Kyiv.: NPU named after M. P. Drahomanov, 2015. – P. 7-11.
5. Kadan A. M. Cloud laboratories for problems penetration testing [Electronic Resource] / A.M. Kadan, A.K. *Doronin*.– Available from: http://ceur-ws.org/Vol-1761/paper24.pdf
6. Korzhova O. V. Theoretical aspects of interdisciplinary communications between mathematical disciplines and disciplines of professional training of future specialists in organization of information security [Electronic Resource] / O. V. Korzhova – Available from: http://fmo-journal.fizmatsspu.sumy.ua/publ/4-1-0-178.
7. Morse N.V. Training of pedagogical personnel for the use of computer telecommunications N.V. Morse // Scientific journal of NPU named after M. P. Drahomanov. Series 2. Computer-oriented educational systems. – K.: NPU named after M. Drahomanov., 2003. – №6.– p. 12-25.
8. Oleksyuk V. P. The application of virtual cloud laboratories in the process of future computer science teachers training / V. Oleksyuk // Scientific journal of NPU named after M. P. Drahomanov. Series 2. Computer-oriented educational systems. – K.: NPU named after M. Drahomanov, 2015. – №1. – p. 76-81.
9. Oleksyuk V. P. Designing of university cloud infrastructure based on Apache CloudStack. [Electronic Resource] / V. Oleksyuk // Information technologies and learning tools. – 2016. – №4. – Available from: http://journal.iitta.gov.ua/index.php/itlt/article/view/1453/1074
10. Evaluation of information and communication competence of pupils and teachers in the conditions of European integration processes in education / V.Yu. Bykov and others.– K. : Pedahohichna dumka, 2017. – 160 p.
11. Ramskyi Yu.S. Professional activity of the teacher in the era of informatization of education [Electronic Resource] / Yu.S. Ramskyi. – Available from: http://enpuir.npu.edu.ua/handle/123456789/9387.
12. Spirin O. M. Methodic of the on-line safety of the senior pupils in the teaching and educational process at school / O.M. Spirin, V.N. Kovalchuk // Information technologies and learning tools, №1(21). – 2011.

DEVELOPMENT OF FUTURE COMPUTER SCIENCE TEACHERS' COMPETENCE OF THE SAFE ACTIVITY IN THE COMPUTER NETWORKS

Vasyl Oleksiuk

Ternopil V. Hnatiuk National Pedagogical University, Ternopil, Ukraine

Abstract. *The article examines the notion of cyber and information security. The author of the scientific and methodological bases of formation of future Informatics teachers ' professional competencies in the field of information security - continuity and phasing. At the first of the specific steps proposed to implement the formation of competences safe activities in the educational information environment of the University. The second stage is to examine students of the theoretical foundations of information security and acquiring skills in application of means of protection of computer networks. Their solution is possible within regulatory disciplines cycle of professional*

training of future teachers of computer science. Third phase of the training proposed to be implemented in the form of a research students their own information systems to identify vulnerabilities and detect unauthorized penetration. The study examined the following components of professional competence of the Informatics teachers: motivational value, organizational and substantial, cognitive-operational and personal-reflective.

Key words: *cyber security, information security, computer science teacher, competence, computer networks.*