УДК 37: 004.56

ВІКТОРІЯ КОВАЛЬЧУК

ПРО ПОКРАЩЕННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЗАГАЛЬНООСВІТНІХ НАВЧАЛЬНИХ ЗАКЛАДІВ

Проаналізовано сучасний стан інформаційної безпеки в загальноосвітніх навчальних закладах і рівень компетентності вчителів інформатики з указаних питань. Розглянуто основні поняття інформаційної безпеки й особливості системи інформаційної безпеки навчального комп'ютерного комплексу. Запропоновано заходи, методи та додаткові засоби з інформаційної безпеки, які забезпечать підвищення надійності програмної складової навчального комп'ютерного комплексу та сприятимуть оптимізації роботи обслуговуючого персоналу.

Ключові слова: *інформаційна безпека, компетентність, комп'ютерний комплекс.*

ВИКТОРИЯ КОВАЛЬЧУК

ОБ УЛУЧШЕНИЯ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕОБРАЗОВАТЕЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ

Дан анализ современного состояния информационной безопасности в общеобразовательных учебных заведениях и уровень компетентности учителей информатики по указанным вопросам. Рассмотрены основные понятия информационной безопасности и особенности системы информационной безопасности учебного компьютерного комплекса. Предложены мероприятия, методы и дополнительные средства по информационной безопасности, которые обеспечат повышение надежности программной составляющей учебного компьютерного комплекса, и будут способствовать оптимизации работы обслуживающего персонала.

Ключевые слова: *информационная безопасность, компетентность, компьютерный комплекс.*

VIKTORIA KOVALCHUK

IMPROVING THE INFORMATION SECURITY AT SECONDARY EDUCATIONAL ESTABLISHMENTS

The research analyses the information security condition at secondary schools and the teachers' competence level in this sphere. The basic concept of information security and features of computer security system of training complex is examined. The measures, methods and the additional means of information security, which will provide the advanced reliability of computer training complex and the optimization of staff activities, are proposed.

Key words: *information security, competence, computer complex.*

Глобальні процеси інформатизації сучасного суспільства, зокрема, загальноосвітніх закладів, загострюють проблеми безпеки шкільних інформаційних систем. Надійність програмної складової навчального комп'ютерного комплексу (НКК) неможливо забезпечити без комплексу адміністративних, організаційних, технічних, процедурних, виховних заходів та програмно-апаратних засобів реалізації цих заходів. Тому проблема комплексного захисту НКК загальноосвітніх навчальних закладів від несанкціонованого втручання є важливою і актуальною. Суперечність між наявним станом інформаційної безпеки в загальноосвітніх навчальних закладах і зростаючою кількістю загроз для шкільних інформаційних ресурсів та систем, вимагають розробки та впровадження комплексної системи інформаціної безпеки навчального комп'ютерного комплексу.

Аналіз наукових досліджень. Становлення наукового напрямку інформаційна безпека, пов'язано з іменами таких видатних учених як М. С. Вертузаєва, В. Ю. Гайковича, В. А. Герасименко, П. Д. Зегжда, В. В. Домарева, В. А. Лужецького, А. А. Малюка, В. В. Хорошко, В. І. Ярочкіна та ін. Однак дослідженню стану інформаційної безпеки (ІБ) в умовах загальноосвітніх навчальних закладів та шляхів застосування методів інформаційної безпеки для покращення надійності програмної складової навчальних комп'ютерних комплексів приділено недостатню увагу.

Метою статті є аналіз, визначення та прогнозування проблем інформаційної безпеки загальноосвітніх навчальних закладів, а також обгрунтування найоптимальніших методів інформаційної безпеки, які дадуть змогу підвищити надійність роботи програмної складової навчальних комп'ютерних комплексів, забезпечать захист інформаційних ресурсів кабінетів інформатики та сприятимуть доцільній організації, оптимізації роботи обслуговуючого персоналу.

Для аналізу стану та визначення проблем інформаційної безпеки у загальноосвітньому навчальному закладі були застосовані теоретичні й емпіричні методи наукового дослідження, зокрема, теоретичні методи — історичний аналіз, аналіз літературних джерел і нормативних документів, порівняння рівня розвитку інформатизації вітчизняних і зарубіжних середніх закладів освіти; прогнозування подальшого розвитку інформатизації школи, а також емпіричні методи дослідження: анкетування, опитування і тестування вчителів і майбутніх учителів інформатики, експертне опитування фахівців з інформаційної безпеки і викладачів інформатики педагогічних ВНЗ.

Завданням першого етапу теоретико-емпіричного дослідження було визначення актуальності проблем інформаційної безпеки в освітній сфері. На даний час спостерігається значний прогрес технологій, зростання швидкості Інтернету, а в найближчому майбутньому більшість шкіл будуть приєднанні до швидкісного Інтернету на постійній основі. Та, незважаючи на значний прогрес комп'ютерно-комунікаційних технологій, використання технології бездротового Інтернету та мобільних пристроїв (ноутбуків) у шкільній освіті, все ще спостерігається значний різнобій у забезпеченні різних шкіл, використання морально застарілого програмно-апаратного забезпечення, не знаходять належної уваги проблеми запобігання доступу дітей до небажаного контенту. До того ж можливості Інтернет-технології не повною мірою використовують у навчанні, а часто їх використання взагалі відволікає дітей від навчального процесу.

Особливої уваги це заслуговує тому, що наслідком підключення до Інтернету є виникнення двох проблем: безпеки дітей у відкритому інформаційному просторі (Інтернет або онлайн безпека дітей) та власне безпеки шкільної інформаційної системи. Тому саме на цьому етапі розвитку шкільної інформатизації, як засвідчує досвід найрозвиненіших країн світу, неможливо обійтися без застосування методів інформаційної безпеки у загальноосвітніх навчальних закладах.

Якщо, наприклад, у США доступ до Інтернету до 2000 року мали всі школи, то в Україні цей процес лише добігає завершення. Крім того, починаючи із середини 90-х років, у США та Європі створюються сайти, суспільні організації та навчально-тренінгові програми для учнів, учителів і батьків, присвячені он-лайн безпеці, то в Україні до цієї проблеми звернулися лише останні 2 роки завдяки зусиллям ряду неурядових і комерційних організацій. Законодавчі та гуманітарні аспекти безпеки дитини в Інтернеті обговорювалися на «круглому столі», який відбувся у Верховній Раді 1 червня 2006 року. Відкриваючи це обговорення, його голова — Михайло Родіонов — зазначив, що проблема безпеки дитини в Інтернеті є важливою і важкою, а досвід України у питаннях безпеки дітей в Інтернеті доволі обмежений [1]. Також відчувається брак україномовних ресурсів з цих питань та недостатня обізнаність учителів інформатики, батьків та інших зацікавлених сторін. Хочеться сподіватися, що участь України не обмежиться проведенням щорічного Дня безпечного Інтернету, а стане системною та виваженою політикою держави в освітній галузі, знайде своє місце у програмах підготовки та перепідготовки вчителів інформатики.

Значним недоліком є також відсутність в Україні будь-якої державної політики щодо застосування у школах спеціальних контент-фільтруючих програм. Для порівняння, у розвинених країнах приділяють значну увагу на державному рівні для розробки і запровадження у школах таких програм, а в Росії така програма розробляється з 2006 року. Держава фінансує не лише

розробку таких програм, але й підтримку бази даних цих програм у актуальному стані. Це дуже важливо, оскільки більшість з цих програми діють за принципом білих і чорних списків і вимагають постійного оновлення, аналогічно до антивірусних програм.

Отже, спостерігається відставання України від розвинених країн у сфері інформатизації, застарілість техніки і програмного забезпечення, недостатня кількість і компетентного обслуговуючого персоналу, не розробленість нормативної бази [4]. Можемо констатувати, що на даний час в Україні склалась ситуація, коли інформаційній безпеці у загальноосвітніх навчальних закладах не приділяється суттєвої уваги. Вкажемо основні причини такої ситуації:

- відсутність служби технічної підтримки, яка забезпечувала б працездатність програмних та апаратних засобів у загальноосвітніх навчальних закладах [4];
- нерозробленість нормативних, правових, законодавчих основ забезпечення інформаційної безпеки в загальноосвітніх навчальних закладах;
- недосконаліть теоретичних та методичних основ застосування методів та засобів наукової галузі інформаційної безпеки в шкільних умовах;
- брак змістовної складової фахової підготовки та перепідготовки вчителів інформатики, зокрема відсутність в ній питань з ІБ.

Якщо подолання перших двох причин можливо лише на державному рівні, на що направлено нещодавно прийняту Концепцію [4], то розв'язання решти проблем має передбачати спільні зусилля науковців і працівників системи освіти.

Завданням другого етапу дослідження було визначення рівня компетентності з інформаційної безпеки учителів інформатики та стану інформаційної безпеки в школах Житомира і Житомирської області.

На початку констатувального експерименту проводилися бесіди з провідними вчителями інформатики Житомира і Житомирської області з метою створення опитувальника. У рамках констатувального етапу експерименту у 2008–2009 роках проводилося анкетування учителів інформатики. Загалом сформовано дві групи опитуваних. Поділ їх на дві групи зумовлений тим, що частина вчителів (перша група, 20 осіб) проходила опитування на ІІІ-му етапі Всеукраїнської олімпіади з інформатики (лютий 2007 року, лютий 2008 року, Житомирська область), на якій вони виступали як члени оргкомітету, входили до складу журі, були керівниками районних, міських та інших команд учнів. Тому таких учителів віднесли до групи експертів, оскільки вони є не лише одними з кращих у Житомирській області, але й відзначаються підвищеним рівнем професійної компетентності з інформаційної безпеки, у своїй професійній діяльності використовують методи інформаційної безпеки. Учителі експертної групи є провідниками передового педагогічного досвіду, для них характерний глибокий і критичний аналіз вивчення нових питань, методик, вони мають високі показники самоосвіти і мотивації застосування методів інформаційної безпеки у загальноосвітніх навчальних закладах. Іншу частину вчителів інформатики (друга група, 40 осіб) було опитано під час проходження курсів підвищення кваліфікації при інституті післядипломної педагогічної освіти, а також на методичних семінарах учителів інформатики у місті Житомирі.

Перша частина анкети була присвячена виявленню стану інформаційної безпеки в загальноосвітніх навчальних закладах, зокрема виявленню основних загроз та методів, які використовують учителі для їх уникнення. Також ми визначили, як використовуються можливості адміністрування наявних операційних систем та чи проводиться резервування, архівування, розмежування доступу до системного та навчального програмного забезпечення і важливої інформації у навчальному комп'ютерному комплексі (НКК). Ще один блок питань був спрямований на з'ясування того, які регламентні та відновлювальні роботи та як часто проводяться у НКК, чи наявне планування таких робіт.

За даними нашого опитування, операційна система Windows XP встановлена на переважній більшості робочих станцій 90% (дані 2008–2009 року), з усіх НКК мережа наявна у 80% класів, а підключення до мережі Інтернет — у 40%. При цьому учні використовують Інтернет на уроках лише у 26% випадках. Незважаючи на доволі задовільні можливості адміністрування ресурсів у вказаній операційній системі, близько 60% учителів не використовують персоналізації взагалі, а лише 40% розділяють користувачів за групами (учні, вчителі). Незважаючи на те, що 54% учителів вказали, що планують регламентні (періодичні) роботи, а 40% вказали, що

такі роботи проводять час від часу, лише у 6% комп'ютерних класів для виконання таких робіт використовують програми-планувальники. Найчастіше серед таких робіт проводять: перевірку на віруси (83%), очистку диску (73%), дефрагментацію (63%), оновлення антивірусних баз (60%), оновлення операційної системи (40%), архівування файлів (30%), створення образу диску (28%).

Серед причин збоїв та відмов учителі вказали: дії учнів (65%), технічні причини (47%), наслідки дій вірусів (42%). Також найчастіше серйозні збої та відмови програмного забезпечення НКК виникають кілька разів на рік (80%), при цьому відволікатися на налагодження комп'ютерів під час уроку вчителям доводиться кілька разів на місяць (47%). Перевірка на віруси жорстких дисків проводиться у НКК найчастіше час від часу (43%), а оновлення антивірусних баз теж найчастіше проводиться час від часу (40%) і 16,5% не проводиться взагалі. Рідко використовуються програми-брандмауери (13%) та програми контролю за діями учнів (16%). Майже ніколи не використовуються повна персоналізація користувачів та мережа на основі сервера, додаткові програми з адміністрування користувачів, а також програми контент-фільтри, хоча така можливість і передбачена нормативними документами [5]. Слабко обізнані вчителі також з поняттям про політику безпеки НКК і не використовують додаткові правила з інформаційної безпеки для користувачів учнів.

У запропонованій анкеті були два схожі запитання: «Чи вважаєте Ви важливими питання інформаційної безпеки у підготовці майбутніх учителів інформатики?» та «Чи вважаєте Ви застосування методів інформаційної безпеки необхідними у вашій професійній діяльності?». На перше питання ствердно відповіли 83% респондентів, 17% сказали «Скоріше так», тоді як на друге ствердно відповіла лише половина респондентів. Порівняння результатів відповідей на ці питання свідчить про розуміння загалом важливості питань інформаційної безпеки у підготовці майбутніх учителів інформатики і про недостатнє розуміння важливості вказаних питань у власній професійній діяльності. Ця обставина вимагає звернути основну увагу на мотивацію та заохочення вчителя інформатики до використання засобів і методів інформаційної безпеки у професійний діяльності.

Порівняння результатів відповідей двох груп респондентів на запитання: «З яких питань інформаційної безпеки Ви хотіли б отримати додаткові відомості?» дає можливість скласти таку таблицю (табл. 1).

Таблиця 1.
Оцінка важливості окремих питань інформаційної безпеки двома групами учителів інформатики

№	Питання	Відсоток ствердних відповідей	
		I-а група	II-а група
1	Безпечна робота в Інтернет і локальній мережі	90%	28%
2	Адміністрування користувачів засобами операційної системи	87%	48%
3	Програмні засоби аварійного відновлення і резервування інформації:	77%	28%
4	Проблеми захисту дітей і підлітків від негативних наслідків інформаційних технологій	76%	40%
5	Організація антивірусного захисту локальної мережі	67%	48%
6	Організація і планування періодичних робіт у кабінеті інформатики	63%	24%
7	Основні поняття інформаційної безпеки	30%	21%
8	Правові та морально-етичні питання інформаційної безпеки	18%	12%
9	Основні поняття криптографії	13%	5%

Загалом, важливість питань інформаційної безпеки у професійній діяльності експерти оцінили вище, ніж контрольна група — відповідно в межах від 90% до 13%, а контрольна група — лише в межах від 48% до 5%. Найбільше турбують учителів інформатики проблеми організації антивірусного захисту локальної мережі (67% і 48%), адміністрування операційних систем і мереж (87% і 48%), захисту учнів (76% і 40%), програмні засоби резервування та віднов-

лення (77% і 28%). Крім того, група експертів на перше місце поставила питання безпеки локальної мережі при підключені до Інтернету — 90% порівняно з 28% у контрольній групі. На перше місце контрольна група поставила питання адміністрування користувачів (48%), що свідчить про вагомі проблеми у цій галузі серед учителів. Незважаючи на те, що необхідність отримання додаткових знань з основних питань інформаційної безпеки вчителі оцінили 30% і 20%, а з морально-етичних і правових питань — 18% і 12%, вважаємо їх вивчення обов'язковими. Що ж до необхідності знань з криптографії у професійній діяльності вчителя інформатики, то переважна більшість учителів вважає їх неважливим (87% і 95%). Графічно результати представлено за допомогою діаграми (рис. 1).

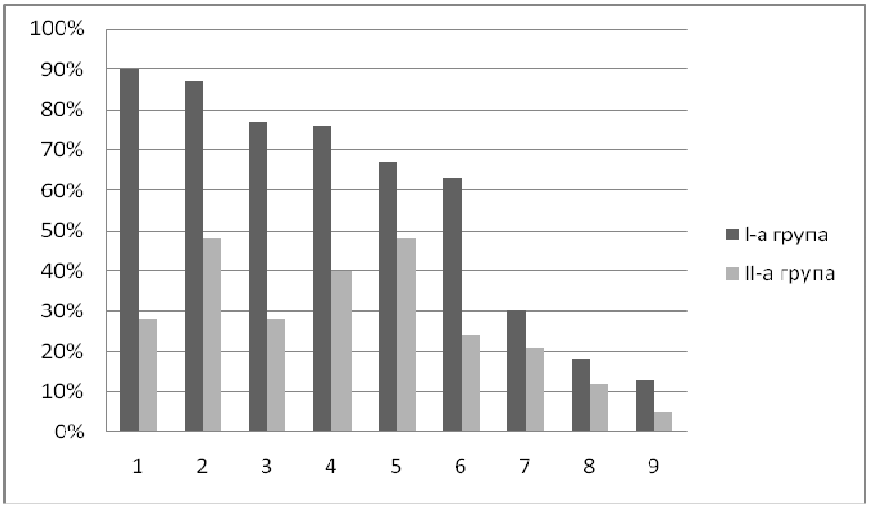

Рис. 1. Важливість питань інформаційної безпеки у професійній діяльності учителів інформатики

Аналіз результатів опитування дозволив виявити стан інформаційної безпеки в загальноосвітніх навчальних закладах і рівень застосування методів інформаційної безпеки вчителями інформатики у професійній діяльності. Результати анкетування дозволяють також зробити висновки про рівень практичних умінь з інформаційної безпеки опитаних учителів інформатики.

Було розроблено модель компетентності з інформаційної безпеки вчителя інформатики, визначено критерії, показники та рівні сформованості вказаної компетентності. Методом діагностування рівня знань і умінь з основ інформаційної безпеки було обрано тест. Розробка тесту проходила в кілька етапів: планування, створення бази предтестових завдань, оцінка та проходження предтестових завдань групою експертів, математична оцінка якості окремих питань, дескрипторів і тесту в цілому, створення кінцевого варіанту тесту. Загалом процедура створення тесту гарантувала валідність тесту як інструменту вимірювання.

Результуючий тест містив 50 запитань з інформаційної безпеки, які обиралися з бази у 100 запитань випадковим чином. Таким чином, результат тестування оцінювався за 50-бальною шкалою. Рівні сформованості професійної компетентності визначалися за результати проходження тесту так: початковий (від 0% до 25% тестових завдань), середній (від 26% до 50%), достатній (від 51% до 75%), високий (від 76% до 100%). Даний тест було використано для вхідного та вихідного контролю під час вивчення спецкурсу «Основи інформаційної безпеки».

На основі розробленого інструментарію (тесту) проводилося вимірювання рівнів сформованості компетентності з інформаційної безпеки за обраними критеріями. Протягом 2008–2010 років виконувалися констатувальні зрізи у двох групах респондентів. До першої групи увійшло 17 учителів інформатики міста Житомира, а до другої — 15 студентів 4-го та 5-го курсу Житомирського державного університету імені Івана Франка спеціальності «Інформатика». Результати констатувального експерименту зображено за допомогою діаграми (рис. 2).

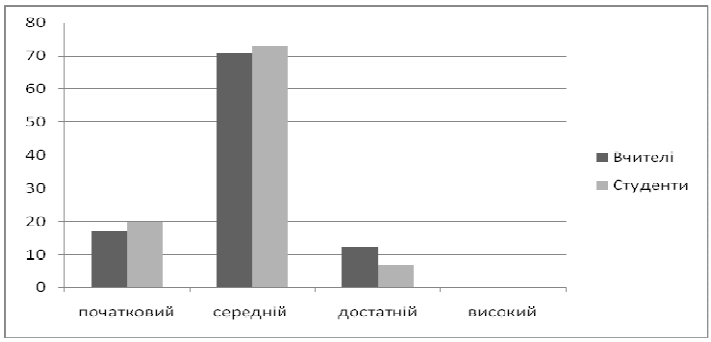

Рис. 2. Порівняльна діаграма рівнів сформованості компетентності з інформаційної безпеки теперішніх і майбутніх учителів інформатики

Як видно з діаграми, більшість респондентів перебувають на середньому і початковому рівнях компетентності з інформаційної безпеки, тоді як для успішного забезпечення інформаційної безпеки кабінету інформатики необхідним є принаймні достатній рівень указаної компетентності. Порівняння результатів тестування двох груп за критерієм U Манна Уітні з достовірністю у 95% відсотків засвідчило, що результати за обома вибірками суттєво не відрізняються. Оскільки на час проведення експерименту учителі інформатики та студенти спеціальності «Інформатика» не вивчали курсу, присвяченого питанням інформаційної або комп'ютерної безпеки (що характеризує ситуацію з вивчення цих питань педагогами загалом в Україні), то робимо висновок, що набуття необхідного рівня вказаної компетентності неможливе без вивчення відповідного курсу у процесі фахової підготовки чи перепідготовки. Досягнення достатнього рівня компетентності шляхом самоосвіти і під час практичної професійної діяльності продемонстровано незначною кількістю протестованих.

Розглянемо, як визначається поняття «інформаційна безпека» у відповідних законодавчих документах.

Інформаційна безпека — стан захищеності життєво важливих інтересів особи, суспільства і держави, при якому запобігається нанесення шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [2].

Найголовнішим завданнями захисту інформації є забезпечення цілісності, конфіденційності та доступності інформації. Виконання цих завдань неможливе без створення комплексної системи захисту інформації. У [3] визначено, що «комплексна система захисту інформації — взаємопов'язана сукупність організаційних та програмно-технічних заходів, засобів та методів захисту інформації». Отже, під системою інформаційної безпеки навчального комп'ютерного комплексу (СІБ НКК), будемо розуміти комплекс заходів: адміністративних, організаційних, технічних, процедурних, виховних та програмно-апаратні засоби реалізації цих заходів. Розглянувши детально вимоги до НКК та види загроз і об'єктів захисту, було створено концептуальну модель СІБ НКК [5]. Згідно цієї моделі обрано такі методи захисту НКК на програмно-апаратному рівні: ідентифікація, автентифікація, авторизація, аудит, розмежування доступу і екранування.

Найбільш значимими для інформаційної безпеки НКК є «програмні засоби захисту, які дозволяють створювати модель захищеної автоматизованої системи з побудовою правил розмежування доступу, централізовано управляти процесами захисту, інтегрувати різні механізми і засоби захисту в єдину систему» [6].

Централізоване управління безпекою, широкий і комплексний захист ресурсів і користувачів, а тому і відповідний рівень безпеки може бути забезпечений лише при організації мережі на основі виділеного сервера. Однак така організація мережі вимагає у складі організації відповідного персоналу: системного адміністратора з відповідним рівнем знань.

У кабінеті інформатики загальноосвітнього навчального закладу доцільно виділити такі напрями захисту: захист ПЗ, антивірусний захист, адміністрування користувачів та захист від загроз Інтернету, централізоване управління безпекою. Виділимо в СІБ НКК такі складові компоненти, кожен з яких відповідає за конкретний напрямок захисту. Ці компоненти дозволять

наочно побачити структуру СІБ НКК на нижнижчому рівні: програмно-апаратному (рис. 3). Зауважимо, що три з цих компонентів повинні бути наявними у будь-якому НКК, а захист від Інтернет загроз необхідний за наявності підключення до мережі Інтернет.

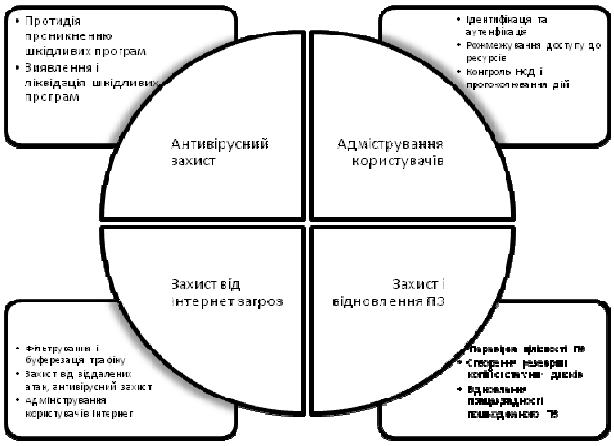

Рис. 3. Структура підсистем СІБ НКК на програмно-апаратному рівні

Централізоване управління є бажаним для підвищення рівня безпеки, але на даному етапі інформатизації школи стикається зі значними труднощами в його реалізації.

Адміністрування користувачів (ідентифікацію, автентифікацію та авторизацію), а також облік (аудит) дій учнів та розмежування доступу до ресурсів можна здійснити засобами сучасних багатокористувацьких операційних систем. Систему аудиту дій користувачів, в основному, використовують для аналізу несанкціонованих (заборонених політикою безпеки) дій (НДС), але її можна використовувати для навчальних цілей.

Для того щоб централізовано управляти процесами захисту, інтегрувати різні механізми і засоби захисту в єдину систему необхідним програмно-апаратно апаратною складовою НКК має бути виділений сервер, на якому має бути встановлена відповідна операційна система. Використання методів адміністрування викликає найбільше труднощів у частині дій персоналу. Реалізація цих методів персоналом неможлива без чіткого планування, організації й відповідної кваліфікації працівників. Так, персоналізація користувачів і ресурсів вимагає підтримання актуальної бази облікових записів великої кількості користувачів, а аудит — налагодження та постійного аналізу системного журналу обслуговуючим персоналом.

Організація антивірусного захисту і резервування програмного забезпечення, застосування методів контент-фільтрації та екранування, адміністрування та розмежування доступу до ресурсів вимагає нагального навчання та підвищення кваліфікації обслуговуючого персоналу. Також оптимізації роботи обслуговуючого персоналу має сприяти: планування та організація заходів інформаційної безпеки в загальноосвітніх навчальних закладах (ЗНЗ), розробка і впровадження політики інформаційної безпеки ЗНЗ, автоматизація регламентних робіт і централізоване управління процесами захисту. Більш докладно дані питання викладено в методичному посібнику [7].

Висновки. Отже, проведене теоретико-емпіричне дослідження свідчить, що питанням інформаційної безпеки у школі приділяється недостатня увага, а проблеми забезпечення інформаційної безпеки в навчально-виховному процесі школи на даний час не розв'язуються. Наявний рівень компетентності вчителів інформатики не дозволяє забезпечити інформаційну безпеку в кабінеті інформатики на належному рівні. Згідно з нещодавно прийнятої Концепцією «Сто відсотків» до 2015 року [4], одним із завдань її впровадження названо «забезпечення інформаційної безпеки та централізованого фільтрування несумісного з навчальним процесом контенту», що дає надію на покращення ситуації з інформаційною безпекою ЗНЗ у найближчому майбутньому.

Перспективи подальших досліджень. Вимагає подальшого дослідження питання мотивації застосування методів інформаційної безпеки у професійній діяльності вчителів інформатики. Необхідно дослідити ефективність розроблених елементів методичної системи форму-

вання та підвищення рівня компетентності з інформаційної безпеки теперішніх і майбутніх учителів інформатики.

ЛІТЕРАТУРА

1. Безпека дитини у Всесвітньому павутинні [Електронний ресурс]. — Режим доступу: http://www.seotm.com/news/Internet/Bezpeka_ditini_u_Vsesv%D1%96tn__omu_pavutinn%D1%96.html
2. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 р. // Відомості Верховної Ради України. — 2007. — №12. — С. 102.
3. Закон України «Про захист інформації в автоматизованих системах» від 05.07.1994 (зі змінами та доповненнями від 31.05.2005) №2594-IV // Відомості Верховної Ради України. — 1994. — №31. — С. 286.
4. Концепція Державної цільової програми впровадження у навчально-виховний процес загальноосвітніх навчальних закладів інформаційно-комунікаційних технологій «Сто відсотків» на період до 2015 року. Затверджено розпорядженням Кабінету Міністрів України від 27 серпня 2010 р. №1722-р. — [Електронний ресурс]. — Режим доступу:http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=1722-2010-%F0
5. Розробка моделі системи захисту інформації навчального комп'ютерного комплексу [Електронний ресурс] / Ковальчук В. Н. Інформаційні технології і засоби навчання: електронне наукове фахове видання. — №3. — 2008. — Режим доступу: http://www.ime.edu-ua.net/em7/emg.html
6. Устенко І. В. Системи захисту інформації: Навч. посібн. / Устенко І. В. — Миколаїв: НУК, 2006. — 68 с.
7. Ковальчук В. Н. Система інформаційної безпеки навчального комп'ютерного комплексу. Методичні рекомендації. / Ковальчук В. Н. — Житомир: ЖДУ. — 2009. — 84 с.