УДК 37:004.73:004.056

Ковальчук Вікторія Наумівна, аспірант Житомирського державного університету імені Івана Франка

РОЗРОБКА МОДЕЛІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ НАВЧАЛЬНОГО КОМП'ЮТЕРНОГО КОМПЛЕКСУ

Анотація

Проаналізовано нормативні документи, які стосуються кабінету інформатики та інформаційно-комунікаційних технологій навчання з погляду інформаційної безпеки. Розроблено модель системи захисту інформації навчально-комп'ютерного комплексу, розглянуто вимоги, принципи побудови, етапи життєвого циклу та ієрархію управління системою захисту інформації. Проведено аналіз типових загроз для інформаційних ресурсів та розглянуто основні методи їх захисту.

Ключові слова: інформаційна безпека, навчальний комп'ютерний комплекс.

Сучасні інформаційні технології надають нові можливості з опрацювання електронних даних та підвищують рівень доступності інформаційних ресурсів для користувача. Однак нові технології опрацювання інформації можуть бути не тільки корисними, але й небезпечними для інформаційних систем та їх власників. З огляду на те, що приватна й ділова інформація має комерційну вартість, важливою є проблема її захисту від несанкціонованого доступу. Електронні дані в освітніх мережах не є виключенням, а тому стають об'єктами випадкових (наприклад, вірусних) та направлених атак. Нині спостерігається тенденція до підвищення кількості атак, які захоплюють контроль над віддаленою системою. Тому проблема комплексного захисту навчальних комп'ютерних комплексів (НКК) загальноосвітніх навчальних закладів від несанкціонованого втручання є важливою й актуальною.

Постає часткова проблема обґрунтувати та розробити модель системи захисту інформації навчально-комп'ютерного комплексу, що й покладено за мету цієї статті.

Для проектування моделі захисту НКК використаємо загально-методичні та науково-практичні підходи, напрацьовані в галузі інформаційної безпеки. Обґрунтування даної моделі будемо базувати на аналізі нормативних документів про кабінет інформатики та інформаційно-комунікаційні технології навчання (КІІКТ).

НКК за своїм призначенням не містить особливо важливої чи конфіденційної інформації, крім власне програмного забезпечення та навчальної інформації. Однак саме програмна частина ННК є найбільш уразливою до помилкових дій недосвідчених користувачів і, поряд з апаратною, саме вона створює передумови безперебійної роботи всього комплексу. Тобто об'єктом захисту виступає не стільки інформація, скільки асоційовані з нею інформаційні ресурси. Забезпечити доступність і цілісність цих ресурсів можна шляхом створення і впровадження комплексної системи захисту інформації (СЗІ) та інформаційних ресурсів НКК. Під СЗІ НКК будемо розуміти комплекс заходів, що спрямовані на забезпечення його інформаційної безпеки. Виходячи зі специфіки НКК, під комплексом заходів будемо розуміти адміністративні, організаційні, технічні, процедурні, виховні та програмно-апаратні засоби реалізації цих заходів. Виконання їх дасть змогу зменшити затрати робочого часу на відновлення програмних збоїв, мінімізувати час простою

непрацюючого програмного забезпечення в навчальний час, підвищити стійкість системи до помилкових дій некваліфікованих користувачів.

Використовуючи термін «інформаційна безпека» (ІБ), будемо вважати, що йдеться про захищеність інформації та інформаційних ресурсів від небажаних впливів, які можуть призвести до неприйнятних втрат суб'єктами інформаційних відносин, зокрема, власниками і користувачами інформації, а також системами її обробки. Збитки можуть носити як моральний (наприклад, розголошення конфіденційної інформації), так і матеріальний (затрати на відновлення працездатності системи, у т. ч. затрати робочого часу) характер [4]. Однак захист інформаційної системи від усіх можливих загроз є економічно недоцільним, тому прийнято встановлювати такий рівень захисту, який мінімізує втрати до прийнятного обсягу.

Розглянемо нормативні документи про кабінет інформатики та інформаційно-комунікаційних технологій навчання в загальноосвітніх навчальних закладах щодо дотримання вимог інформаційної безпеки.

У «Положенні про кабінет інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів» зазначено, що основною метою створення КІІКТ є забезпечення належних умов для проведення навчально-виховного процесу; навчально-виховне середовище, створене КІІКТ, використовується для навчання інформатики та інших навчальних дисциплін…» [9:3]. Навчально-виховне середовище безпосередньо створює навчально-комп'ютерний комплекс, під яким розуміють сукупність програмно-апаратних засобів КІІКТ, як зазначено в методичних рекомендаціях щодо облаштування і використання кабінету інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів [8:10]. Отже, НКК має забезпечувати якісний безперервний процес навчання. Тому основною вимогою до НКК є надійність роботи апаратної та програмної його частин. У документі [8:19, 28] регламентовано вимоги до надійності програмно-апаратного забезпечення.

Технічні відмови, збої та відповідний ремонт обладнання детально прописані в названих документах, однак щодо збоїв у програмному забезпеченні, то цьому питанню приділено значно менше уваги. Відмови і збої НКК зумовлені не тільки апаратною, але й програмною його частиною. У роботі [8] вказано, що «…встановлення програмного забезпечення та налагодження програмних засобів здійснюється працівниками навчальних закладів». Очевидно, що ліквідовувати збої у роботі програмного забезпечення мають ті ж самі працівники. З аналізу нормативних документів [8:19] та [9:7] випливає, що роботи з підтримки працездатності програмної складової НКК та захисту його від загроз є недостатньо регламентованими, а саме, не вказано, хто і як планує та проводить регламентні роботи. Вбачається за доцільне, що планування робіт у вигляді річного календарного плану регламентних робіт повинен проводити зав. лабораторії (учитель інформатики), а їх виконання – лаборант. У правилах роботи учнів в КІІКТ [8:26] до правил інформаційної безпеки відносяться лише заборона приносити та використовувати носії даних без дозволу вчителя, а також правила поводження учнів у випадку аварійної зупинки. Ці правила необхідно доповнити вимогами поводження з навчальною інформацією та програмною складовою НКК. Доповнення до правил повинні розроблятися зав. лабораторії, з огляду на прийняту КІІКТ політику інформаційної безпеки.

Для розробки теоретичної моделі СЗІ НКК врахуємо загальні етапи проектування систем захисту [6: 18]. Насамперед проведемо аналіз безпеки середовища, тобто визначимо основні загрози для НКК, їх джерела, а також предмет захисту. У нормативних документах [2, 8, 9, 10] основними

загрозами вважаються відмова і збій програмно-апаратного забезпечення та помилкові дії користувачів. Опитування вчителів інформатики ЗНЗ Житомирської області (30 респондентів), що проводилось у 2008 році, показали, що переважна більшість вчителів (63%) вважає, що частота серйозних збоїв та відмов НКК становить декілька разів на рік. Серед причин збоїв та відмов програмного забезпечення (ПЗ) вчителі назвали: дії учнів – 83%, вірусів – 36%, технічні причини – 30%.

НКК за своїм призначенням використовується в основному не як система автоматизованої обробки інформації, а як навчальне середовище. Тому інформацію, що міститься в НКК, за рівнем важливості та необхідності захисту доцільно розподілити так: конфіденційна інформація (паролі тощо); важлива інформація (навчальна та звітна); неважлива (тимчасові файли та файли учнів). Конфіденційна інформація потребує шифрування, важлива – резервування, неважлива – періодичного знищення.

Використовуючи модель типового НКК, схематично (рис. 1) зобразимо на ній види загроз та їх джерела. Зазначимо, що НКК містить від 4 до 15 комп'ютерів.

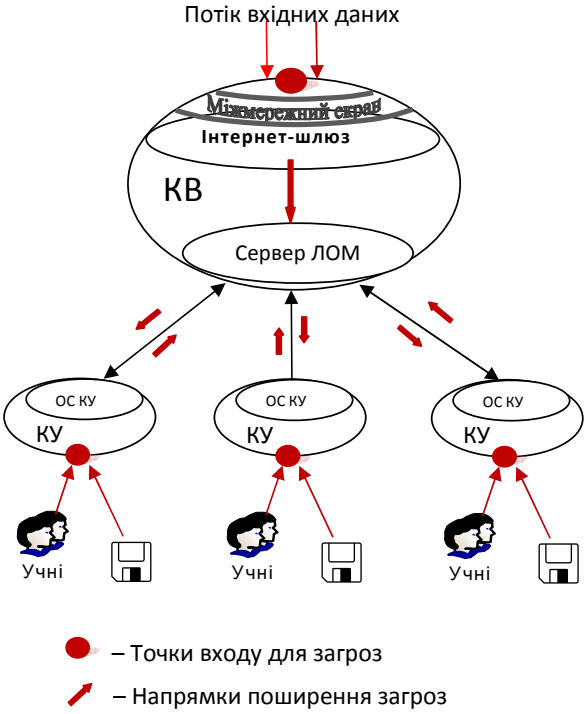

Рис. 1. Види загроз та їх джерела для типового навчального комп'ютерного комплексу

Примітка. ЛОМ – локальна обчислювальна мережа; КУ – комплект учня; КВ – комплект вчителя; ОС – операційна система. (Рис. 1).

До основних загроз належить (у порядку спадання вірогідності):

Основні загрози

- Помилкові, несанкціоновані дії.
- Проникнення шкідливих програм.
- Збої та відмови.
- Помилки, лазівки, нестійкість.
- Віддалена атака.

Джерела загроз

- Користувачі.
- Змінні носії, Інтернет.
- Поломки обладнання.
- Програмне забезпечення (ПЗ).
- Інтернет.

Безперебійне функціонування НКК неможливе без захисту його програмної складової, яка у

своїй сукупності ці функції реалізує. Тому за рівнем критичності для навчального процесу, відповідної складності і трудомісткості відновлення потрібно ранжирувати таке програмне забезпечення:

- системне програмне забезпечення;
- навчальне програмне забезпечення;
- інші програми.

Основною вимогою, що висувається до апаратно-програмного забезпечення кабінету інформатики, є його інформаційна надійність і стійкість до помилкових дій користувачів-учнів. Під інформаційною надійністю розуміють стійкість інформаційної системи і/або її складових щодо факторів впливу, які є зовнішніми відносно системи [8:10]. Визначення надійності дається через стійкість, однак не визначається, що таке стійкість, а також не вказані критерії її визначення і методи забезпечення. У «Великому тлумачному словнику сучасної української мови» «стійкий» визначається як «здатний витримувати зовнішній вплив, протидіяти чомусь; здатний зберігатися, існувати за несприятливих умов» [1:1196]. Очевидно, що значна кількість недосвідчених користувачів створює «несприятливий зовнішній вплив» для НКК. І цей вплив, в основному, спрямований на програмне забезпечення. Відзначимо, що жодне програмне забезпечення не може апріорі володіти абсолютною надійністю, стійкістю щодо помилкових дій користувачів. Тому забезпечувати стійкість ПЗ до помилкових дій значної кількості недосвідчених користувачів потрібно додатковими заходами та засобами, а саме СЗІ НКК.

Мета створення СЗІ НКК – підвищити надійність програмної складової СЗІ НКК у разі помилкових дій значної кількості недосвідчених користувачів та інших вірогідних загрозах.

Основні труднощі реалізації системи захисту полягають у тому, що вона повинна задовольняти дві суперечливі вимоги: з одного боку, забезпечувати надійність роботи інформаційної системи, а з іншого, – система захисту не повинна створювати помітних незручностей під час роботи користувачів з ресурсами системи [9:9]. Рекомендації [8: 12] можемо покласти в основу вимог до засобів захисту типової НКК.

Загальні завдання СЗІ НКК:

- підвищувати загальну надійність роботи НКК;
- забезпечувати комплексний захист від найбільш вірогідних загроз;
- здійснювати виховний вплив на користувачів-учнів.

Організаційні вимоги до СЗІ НКК:

- максимально використовувати можливості наявного програмного забезпечення НКК для захисту;
- зменшити час простою НКК за рахунок мінімізації програмних збоїв та відмов;
- зменшити трудомісткість відновлювальних робіт;
- бути максимально автоматизованою, простою та регламентованою для персоналу;
- бути максимально комфортною для користувачів;
- не вимагати від персоналу компетентностей, що виходять за межі їх посадових обов’язків.

Вимоги до програмно-апаратної складової СЗІ НКК:

- створювати єдиний комплекс засобів, що захищає НКК від всіх вірогідних загроз;
- захищати програмну складову НКК від випадкових неправильних дій учня або вчителя

(користувача) та від інших несанкціонованих дій;

- забезпечувати персоналізацію користувачів і ресурсів системи;
- вести облік використання ресурсу кожного комп'ютера, комплексу в цілому та мережі Інтернет;
- протоколювати завдання, які виконані на кожному робочому місці.

На основі аналізу задач та вимог до СЗІ, а також джерел [5, 6, 11] ***принципи*** побудови СЗІ НКК є такими:

- *Системність*. Системний підхід вимагає врахування всіх взаємопов'язаних, взаємодіючих і змінних у часі елементів, умов та факторів, що суттєво впливають на розуміння та рішення проблеми безпеки ІС.
- *Комплексність*. Цей підхід полягає у тому, що у разі використання максимально можливого спектру заходів, засобів і методів необхідно їх погодження для створення цілісної системи захисту, що перекриває всі можливі шляхи реалізації загроз і не має слабких місць у разі поєднання різнорідних компонентів.
- *Виховна спрямованість*. Під час розробки та реалізації комплексної СЗІ НКК у першу чергу слід обирати ті методи та засоби, які справляють найбільший виховний вплив на користувачів-учнів. Необхідною складовою системи захисту є цілісний комплекс виховних заходів, що спрямований на формування в учнів свідомого ставлення до правил інформаційної безпеки та їх безумовне виконання.
- *Надійність*. Необхідно забезпечити неможливість зниження рівня надійності у разі виникнення в системі збоїв, відмовлень, навмисних дій порушника або ненавмисних помилок користувачів і обслуговуючого персоналу.
- *Постійність захисту*. Захист НКК є регулярним цілеспрямованим процесом, що здійснюється на всіх етапах життєвого циклу СЗІ.
- *Принцип мінімізації привілеїв*. Цей принцип полягає у виділенні користувачам тільки тих привілеїв, що є необхідними для виконання їх безпосередніх обов'язків і забезпечує права, які необхідні для виконання навчальних завдань.
- *Доцільність*. СЗІ повинна забезпечувати такий рівень захисту ресурсів системи, який зменшує до прийнятних розмірів відмову у доступі до ресурсів системи, що є результатом програмних збоїв та відмов. З іншого боку, витрати часу на експлуатацію системи захисту НКК не повинні перевищувати витрат часу на ліквідацію програмних збоїв та відмов під час експлуатації НКК без системи захисту інформаційних ресурсів.
- *Адаптованість*. СЗІ повинна бути достатньо легко адаптованою до змін вимог захисту та інших змін програмно-апаратного забезпечення НКК, що виникають в період її експлуатації.
- *Простота і керованість*. Проста й керована архітектура системи дає можливість перевірити погодженість конфігурації різних компонентів і здійснити централізоване адміністрування. Прості у використанні механізми захисту не вимагають надмірних затрат на освоєння та експлуатацію.
- *Загальна підтримка заходів безпеки*. Ефективність СЗІ значною мірою залежить від усвідомлення необхідності її використання та сприяння заходам безпеки з боку всього персоналу: від керівника школи до лаборанта.

Система захисту інформації НКК створюється людьми (персоналом) і для людей (учителів та

учнів). Тому вона є, перш за все, соціотехнічною системою. Успішне створення і функціонування СЗІ НКК неможливе без врахування навчально-виховної взаємодії учителя та учнів, що опосередкована засобами НКК. Врахування особливостей СЗІ НКК повинно забезпечуватися поєднанням підходів ІБ, перш за все, впровадженням продуманої політики інформаційної безпеки КІІКТ, а також педагогічних підходів до виховання дисциплінованого учня-користувача, де під політикою інформаційної безпеки розуміється набір законів, правил, практичних рекомендацій і практичного розвитку, що визначають управлінські та проектні рішення в галузі захисту інформації [**Ошибка! Источник ссылки не найден.**: 101]

Комплексний підхід до інформаційної безпеки вимагає використання сукупності заходів відносно користувачів-учнів, а саме: контроль з боку вчителя (перш за все, візуальний), контроль і реагування на несанкціоновані дії (НСД) програмних засобів захисту, реагування персоналу та застосування вчителем адекватних виховних заходів у разі виникнення НСД. Несанкціонованими вважаються дії, що заборонені політикою безпеки КІІКТ і конкретизовані у правилах роботи користувачів.

Під час організації заходів з інформаційної безпеки особливо важливим є планування і проведення комплексу взаємопов’язаних заходів на всіх етапах життєвого циклу СЗІ НКК. Під життєвим циклом системи захисту інформації розуміються всі етапи її проектування, впровадження й експлуатації від початку створення до переходу на іншу програмно-апаратну платформу.

Враховуючи специфіку НКК як навчального середовища, візьмемо за базовий період життєвого циклу навчальний рік. Більшість процедурних заходів є періодичними, наприклад, процеси створення й оновлення резервних копій, знищення залишкової інформації, оновлення бази облікових записів (видалення старих і створення нових), оптимізації роботи ПЗ. Планування регламентних робіт слід узгоджувати не лише з періодом навчального року, але й з навчальним планом та навантаженням на лабораторію. Завідувачем лабораторії кожен навчальний рік повинен розроблятися детальний календарний план регламентних робіт, у якому вказується дата і час їх проведення. Регламентні роботи виконуються лаборантом і контролюються зав. лабораторії. Вони складають основу безперервного циклу захисту інформації НКК (рис. 2).

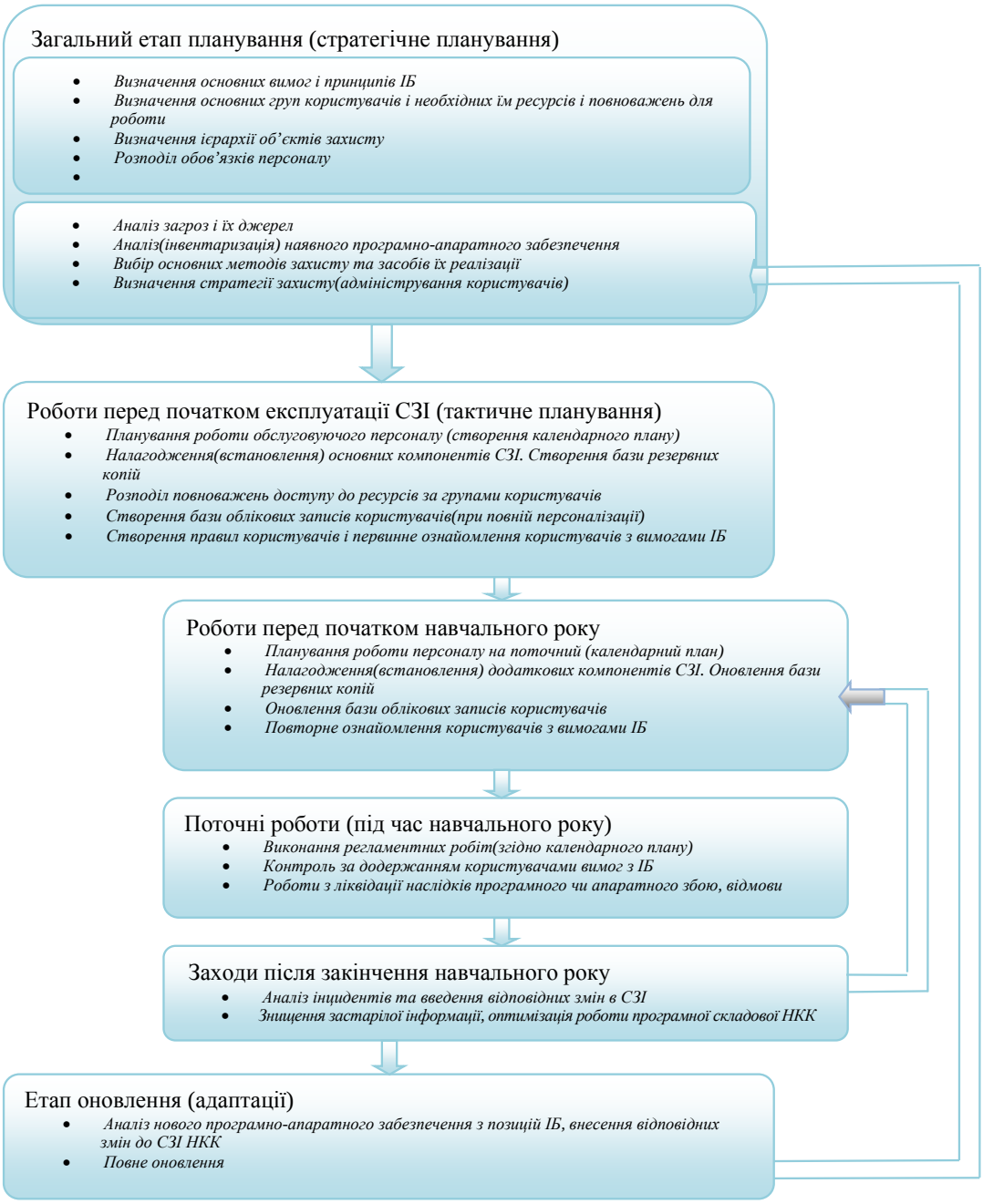

Рис. 2. Заходи з інформаційної безпеки на всіх етапах життєвого циклу системи захисту інформації навчального комп'ютерного комплексу

Оскільки життєвий цикл СЗІ в основному співпадає з життєвим циклом інформаційної системи (ІС), то більшість спеціалістів з інформаційної безпеки вважають, що найбільшої ефективності СЗІ можна досягти лише у разі одночасної розробки ІС та її системи захисту. Це вимагає врахування вимог до інформаційної безпеки НКК загальноосвітніх навчальних закладів на державному рівні, оскільки це дозволить добирати ефективні, з точки зору захисту НКК, програмно-апаратні засоби ще на етапі закупівлі й сертифікації обладнання і програмного забезпечення.

Система захисту інформації як складова новітніх інформаційних технологій має відносно короткий життєвий цикл, відповідний часу зміни програмно-апаратної платформи ІС. Швидкість оновлення вимагає розробки методології створення СЗІ, в основу якої закладені принципи простого перенесення на іншу програмно-апаратну платформу. Таку основу складає комплексна система

заходів, яка за правильної розробки може бути перенесена на іншу платформу з найменшими втратами.

Комплексна система захисту інформації сприймається як взаємопов'язана сукупність заходів, засобів та методів захисту. Використовуються різні підходи до визначення сукупності заходів, засобів та методів захисту. Виходячи зі специфіки навчальних інформаційних систем, виберемо найбільш прийнятні види заходів: нормативно-законодавчі, адміністративні, організаційні, виховні, технічні, а також програмно-апаратні засоби.

Система заходів реалізується в основному персоналом школи, тому важливим є розподіл відповідальності між персоналом за проведення відповідних видів заходів, а також виявлення ієрархії управління системою комплексних заходів з ІБ (рис. 3). Запропонований підхід дозволяє представити сукупність заходів та засобів у вигляді системи рівнів, кожний з яких підпорядкований попередньому і керує іншим.

Нормативно-законодавчі заходи – це сукупність законів і нормативних документів, що діють у галузях освіти та інформаційної безпеки, на яких базується правове регулювання питань, пов'язаних з безпекою інформації та інформаційних систем у загальноосвітніх навчальних закладах. Зазначимо, що нормативно-законодавче поле у цій галузі врегульоване ще недостатньо.

Адміністративні заходи реалізуються керівництвом школи і спрямовані на вирішення стратегічних питань в галузі інформаційної безпеки. Організаційні заходи спрямовані на створення, експлуатацію та оновлення СЗІ НКК. Технічні заходи реалізують безвідмовне функціонування обладнання СЗІ НКК. Поточне функціонування СЗІ НКК неможливе без реалізації процедурних заходів, під якими розуміють всі періодичні регламентні роботи з інформаційної безпеки. Виховні заходи полягають у системному підході до виховної роботи з учнями та сприяють формуванню у них компетентності з інформаційної безпеки та безумовному виконанню правил ІБ. Програмно-апаратні засоби – це вся сукупність засобів НКК, яка реалізує СЗІ на програмно-апаратному рівні.

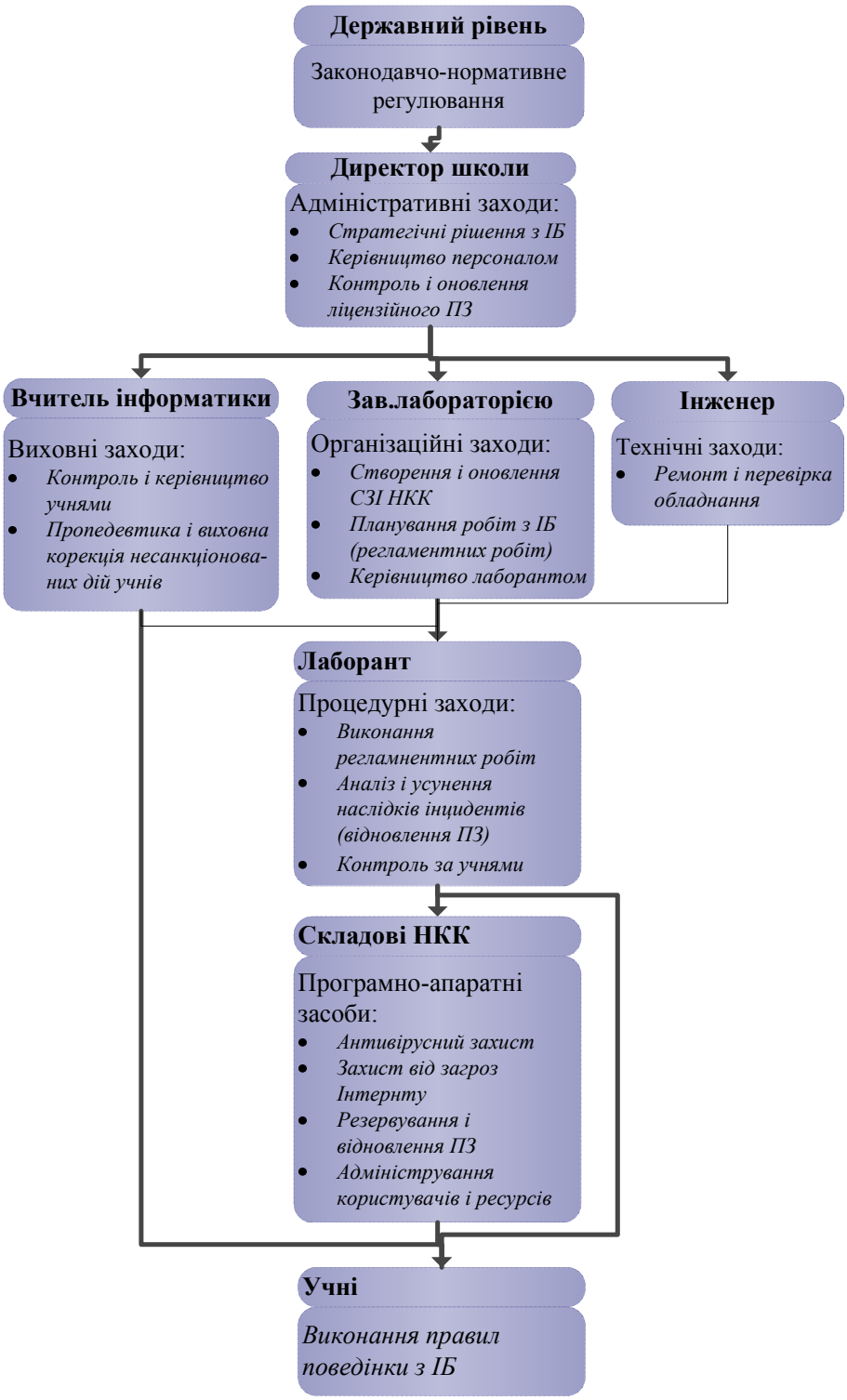

Рис. 3. Управління системою захисту інформації навчального комп'ютерного комплексу

Досить часто розглядають теоретичну модель системи захисту, де під перешкодою розуміють однорідну захисну оболонку, до якої поміщений предмет захисту. У роботі [7:116–124] розглядаються такі види моделей захисту: елементарна, багатоланкова та багатошарова. Пропонуємо багатошарову модель СЗІ НКК, у якій показано взаємозв'язок таких компонентів, як загрози, захисні заходи, програмно-апаратні засоби та предмет захисту (рис. 4). Програмно-апаратні засоби є частиною інформаційної системи (НКК), а сукупність заходів реалізується персоналом школи. Зазначимо, що сукупність заходів і програмно-апаратних засобів «перекривають» всі можливі загрози.

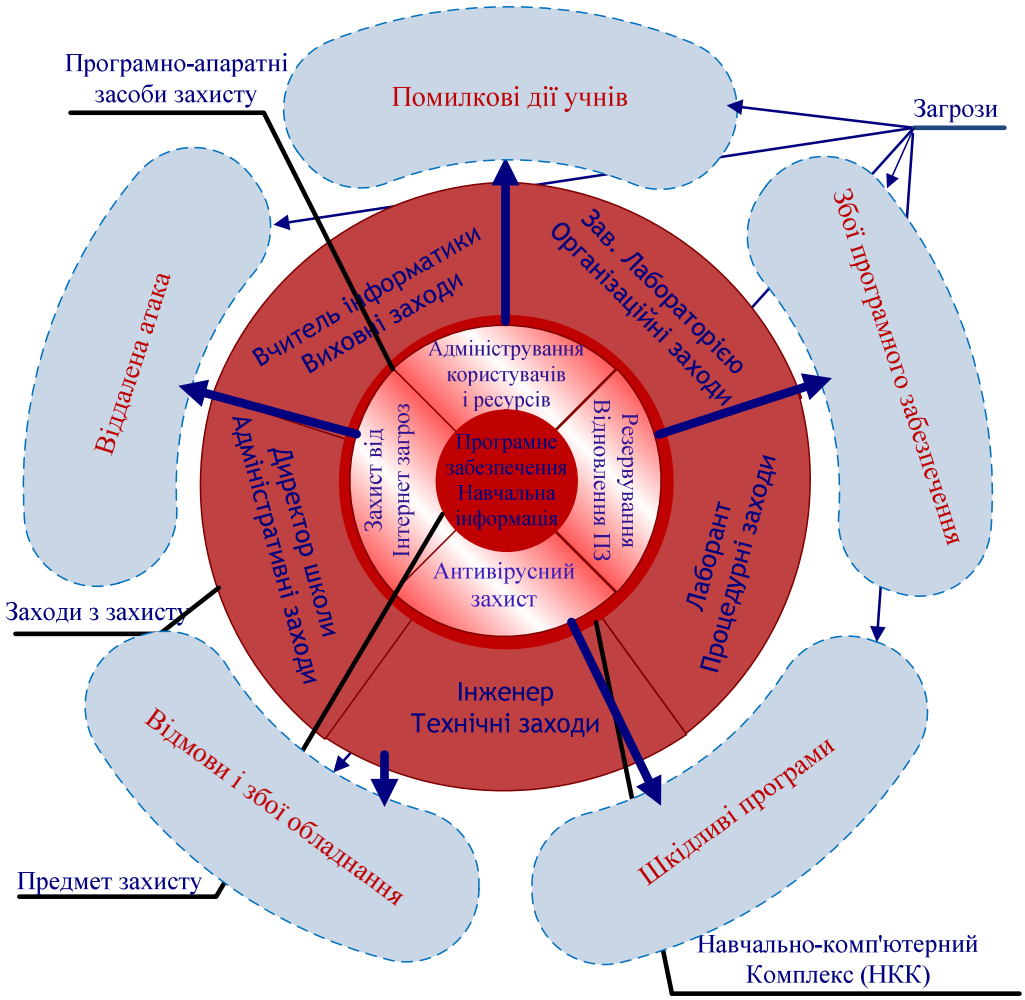

Рис. 4. Модель системи захисту навчального комп’ютерного комплексу

Окремо взяті технічні чи програмні засоби не можуть діяти без організованої та спрямованої діяльності всіх учасників інформаційних взаємодій, без регламентації, розробки і впровадження правил інформаційної безпеки (політики безпеки), постійного керівництва обслуговуючим персоналом і керуванням системою безпеки НКК. «Всі зусилля по забезпеченню внутрішньої безпеки комп’ютерних систем фокусуються на створенні надійних і комфортних механізмів регламентації дій всіх законних користувачів і обслуговуючого персоналу та присилування їх до безумовного виконання встановленого в навчальному закладі режиму доступу до ресурсів системи. Організаційні заходи необхідні для забезпечення ефективного виконання інших заходів захисту в частині, що стосується регламентації дій людей» [3:31]. Оскільки на даному етапі інформатизації загальноосвітніх навчальних закладів є труднощі з виділенням коштів на закупівлю та оновлення саме програмно-апаратних засобів, то для захисту НКК можемо використовувати лише наявні їхні можливості. Найбільш перспективним будемо вважати максимальне використання організаційних, процедурних та виховних заходів для підвищення ефективності СЗІ НКК, які не вимагають додаткових коштів. Саме комплексний підхід до інформаційної безпеки НКК, усвідомлення необхідності таких заходів на всіх рівнях управління освітою, навчання та підвищення компетентності обслуговуючого персоналу та вчителів інформатики є запорукою успішної реалізації вимог, висунутих до надійності програмної складової НКК.

Розглянувши детально вимоги до НКК та види загроз і об’єктів захисту, а також враховуючи

наявні засоби та програмно-технічне забезпечення типового НКК, спробуємо навести найбільш прийнятні методи захисту НКК:

- ідентифікація (найменування і розпізнання), аутентифікація (підтвердження достовірності), авторизація (надання повноважень) суб'єктам, протоколювання та аудит дій користувачів;
- розмежування (контроль) доступу до ресурсів.
- облік та аналіз подій, що відбуваються в системі.
- контроль цілісності і резервування критичних ресурсів системи.

Зі всього вище викладеного можемо зробити такі висновки.

На основі аналізу нормативних документів обґрунтовано мету, завдання та вимоги до СЗІ НКК, а також сформульовано принципи її побудови. Мета СЗІ НКК полягає у підвищенні надійності програмної складової НКК, доступності інформаційних ресурсів та цілісності програмного забезпечення. Ефективне функціонування СЗІ НКК можливе лише за комплексного поєднання нормативно-законодавчих, адміністративних, організаційних, технічних, процедурних, виховних заходів та можливостей наявних програмно-апаратних засобів НКК.

Розглянуто взаємозв'язок таких складових компонентів СЗІ НКК та середовища її експлуатації, як види загроз та їх джерел для типового НКК, заходів захисту та етапів життєвого циклу, обов'язків персоналу та рівнів управління СЗІ НКК, на основі чого побудовано модель системи захисту інформації навчального комп'ютерного комплексу.

Запропонована модель може бути застосована:

- *для розробки практичної СЗІ НКК*. Оскільки обладнання КІІКТ, склад персоналу, умови експлуатації загалом є типовими, то дана модель може слугувати зразком під час створення конкретної СЗІ НКК. Також відпадає необхідність у повторному проведені деяких етапів проектування, таких як аналіз середовища експлуатації, визначення мети, вимог, принципів побудови НКК, добір напрямків, заходів, методів захисту тощо;
- *для навчання майбутніх учителів інформатики*. Використання моделі в курсі інформаційної безпеки для майбутніх учителів інформатики буде сприяти узагальненню та систематизації знань з ІБ, формуванню системного підходу до проблем захисту НКК.

Подальшої розробки і дослідження вимагають такі питання:

- розробка основних положень політики інформаційної безпеки КІІКТ загальноосвітніх навчальних закладів та правил інформаційної безпеки для учнів;
- уточнення виховних, процедурних і організаційних заходів СЗІ НКК;
- конкретизація і приблизне календарне планування регламентних робіт з ІБ;
- створення алгоритму дій персоналу під час ліквідації програмних відмов і збоїв;
- практична перевірка ефективності запропонованої моделі СЗІ НКК.

Список використаних джерел

1. Великий тлумачний словник сучасної української мови / [Уклад. і гол. ред. В.Т. Бусел. – К.; Ірпінь: ВТФ «Перун», 2004. – 1440 с.

2. Вимоги до специфікації навчальних комп'ютерних комплексів // Комп'ютер у школі та сім'ї. – 2007. – № 4. – С. 50–51.

3. *Гайкович В.Ю*. Основы безопасности информационных технологий: учебн. пособие / Гайкович В.Ю., Ершов Д. В. – Москва: Изд-во МИФИ, 1995. – 93 с.

4. *Галатенко В.А.* Основы информационной безопасности: Учеб. курс [Электронный ресурс] / В. А. Галатенко // Веб-сайт Интернет-университета информационных технологий. – 2003. – Режим доступу http://www.intuit.ru/department/security/secbasics/.

5. *Домарев В.В.* Защита информации и безопасность компьютерных систем / Домарев В. В. – К.: Изд-во «Диа-Софт», 1999. – 480 с.

6. *Лужецький В. А.* Основи організаційного захисту інформації :[Навч. посіб.] / В.А. Лужецький, Л.І. Северин, П.Ю. Гульчак, А.Д. Кожухівський. – Вінниця: ВНТУ, 2005. – 148 с.

7. *Мельников В. В.* Защита информации в компьютерных системах. / Мельников В.В. – М.: Финансы и статистика; Электроинформ, 1997. – 368 с.

8. Методичні рекомендації щодо облаштування і використання кабінету інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів // Інформатика. – 2005. – № 2–3. – С. 9–32.

9. Положення про кабінет інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів // Інформатика. – 2005. – №2–3. – С. 3–8.

10. Правила безпеки під час навчання в кабінетах інформатики навчальних закладів системи загальної середньої освіти // Інформатика. – 2005. – № 2–3. – С. 33–37.

11. *Устенко І.В.* Системи захисту інформації: Навч. посіб. / Устенко І.В. – Миколаїв: НУК, 2006. – 68 с.

РАЗРАБОТКА МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ УЧЕБНОГО КОМПЬЮТЕРНОГО КОМПЛЕКСА

Ковальчук В.Н.

Аннотация

Проанализированы нормативные документы, которые относятся к кабинету информатики и информационно-коммуникационным технологиям обучения с точки зрения информационной безопасности. Разработана модель системы защиты информации учебно-компьютерного комплекса, а именно: рассмотрены требования и принципы построения, этапы жизненного цикла и иерархию управления системой защиты информации. Проведен анализ типичных угроз для информационных ресурсов и предложены основные методы их защиты.

Ключевые слова: информационная безопасность, учебный компьютерный комплекс.

DEVELOPING OF THE SYSTEM INFORMATION SECURITY MODEL FOR COMPUTER TRAINING COMPLEX

Kovalchuk V.

Resume

The regulatory documents regarding the computer training rooms and information communication technologies in respect to the information safety are being analyzed in the given paper. The model of information security system of the computer training complex is developed. In particular there are considered the requirements to the security system construction, its functioning and the stages of the lifecycle. The analysis of typical risks for the information resources is conducted, the main methods of their information security are offered.

Keywords: information security, computer training complex.