УДК 004:37

ОРГАНІЗАЦІЯ РОБОТИ КАБІНЕТУ ІНФОРМАТИКИ В ЗАГАЛЬНООСВІТНЬОМУ НАВЧАЛЬНОМУ ЗАКЛАДІ З УРАХУВАННЯМ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Ковальчук В.Н.
Житомирський державний університет імені Івана Франка, Україна

В роботі розглянуто питання застосування організаційних заходів з інформаційної безпеки в загальноосвітньому навчальному закладі, зокрема запропоновано приблизний календарний план регламентних робіт.

Ключові слова: *інформаційна безпека, кабінет інформатики, загальноосвітній навчальний заклад.*

Комплексна система інформаційної безпеки навчального комп'ютерного комплексу (СІБ НКК) розуміється як взаємозалежна сукупність заходів, засобів і методів захисту. Використовуються різні підходи до визначення сукупності заходів, засобів і методів захисту. З огляду на специфіку функціонування навчальних інформаційних систем, найбільш прийнятними є такі види заходів: нормативно-законодавчі, адміністративні, організаційні, процедурні, виховні, програмно-технічні.

Надійність і безперебійність роботи НКК неможливо реалізувати лише самою наявністю програмно-апаратних засобів захисту. Так, наприклад, антивірусний захист не може бути вичерпаний лише встановленням антивірусного пакету на робочі станції учнів і комп'ютер вчителя, це є комплексна система організаційних і програмно-технічних заходів. Захист програмної складової НКК від можливих загроз вимагає також чіткого планування та виконання регламентних робіт обслуговуючим персоналом, що є важливою складовою організаційних заходів захисту.

Окремо взяті технічні чи програмні засоби не можуть бути використанні без організованої і цілеспрямованої діяльності всіх учасників інформаційних взаємодій, без регламентації, розробки та впровадження правил інформаційної безпеки (політики безпеки), постійного керівництва обслуговуючим персоналом і управлінням системою безпеки НКК. "Усі зусилля щодо забезпечення внутрішньої безпеки комп'ютерних систем фокусуються на створенні надійних і комфортних механізмів регламентації дій всіх законних користувачів і обслуговуючого персоналу і примушення 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, яка стосується регламентації дій людей [1, 31]". Оскільки на сучасному етапі інформатизації загальноосвітніх навчальних закладів є труднощі з закупівлею або оновленням програмно-апаратних засобів, то для захисту НКК можна використовувати лише наявні в них засоби. Тому найбільш перспективним вбачається максимальне використання організаційних та виховних заходів з підвищення ефективності СІБ НКК, впровадження яких не потребує витрати додаткових матеріально-технічних ресурсів та інших засобів. Саме комплексний підхід до інформаційної безпеки НКК, усвідомлення необхідності таких заходів на всіх рівнях управління освітою, навчання та підвищення компетентності обслуговуючого персоналу і вчителів інформатики є запорукою успішної реалізації вимог, висунутих до надійності функціонування програмної складової НКК.

Робота кабінету інформатики має свою специфіку порівняно з іншими лабораторіями та кабінетами школи. Для того щоб підвищити ефективність роботи обслуговуючого персоналу, необхідно розробити нові підходи до організації роботи НКК. Використання таких підходів дозволить застосувати методи інформаційної безпеки для підвищення надійності програмного компоненту НКК, зменшити витрати робочого часу на відновлення

його працездатності під час програмних збоїв, підвищить захищеність програмної складової НКК.

Серед основних методів, які використовуються для підвищення захищеності та відновлюваності програмної складової інформаційної системи (ІС), є резервування і періодична перевірка її цілісності. Ці методи можуть реалізовуватися системними утилітами, які входять до складу операційної системи або іншими програмами, наприклад антивірусними. При першому запуску цих програм створюється база відповідних значень незмінних файлів, зокрема системних (наприклад контрольних сум); при повторному запуску здійснюється перевірка всіх незмінних файлів на модифікацію. Якщо така модифікація здійснена, то це може свідчити про наявність вірусів або може бути результатом дій недосвідчених користувачів. Програми-ревізори, як правило, можуть відновлювати пошкоджені файли. Однак, якщо ці ушкодження досить значні, зачіпають критично важливі файли операційної системи, то для їх відновлення необхідно мати резервну копію системної області жорсткого диска. Системні утиліти, які створюють архіви-образи логічних дисків допомагають швидко відновити роботу пошкодженої операційної системи не перевстановлюючи її. Необхідною умовою використання цих засобів є чітке планування та виконання регламентних робіт персоналом. Наприклад, образ системного диска обов'язково робиться як мінімум раз на навчальний рік після відповідних підготовчих робіт, а перевірка файлів на цілісність може проводитися періодично.

Методи оптимізації і підвищення надійності роботи кабінету інформатики та інформаційно-комунікативних технологій навчання (КІІТК).

Резервування є основним методом боротьби із наслідками збоїв та підвищення надійності ІС. Воно буває як програмне так і апаратне. В умовах школи мова може йти лише про резервування системного програмного забезпечення, та іншої важливої інформації. Пропонується проводити резервування системної області жорсткого диску принаймні на початку кожного навчального року. Питання про необхідну кількість резервних копій (чи така копія робиться для кожного комп’ютера учня окремо чи одна для всіх комплектів учня (КУ)) вирішується проведенням уніфікації.

Уніфікація. Як правило, програмно-апаратне забезпечення кожного робочого місця учня є стандартним. Тобто на них встановлено однакові операційні системи, інші прикладні програми. Однак під часом експлуатації дана ідентичність щезає, змінившись різнорідністю, яка збільшує затрати часу на обслуговування КУ. Для того щоб забезпечити ідентичність КУ під час експлуатації, пропонуються такі заходи.

Первинна уніфікація. Якщо апаратні складові КУ є однаковими чи з незначними відмінностями, то можливе створення єдиної резервної копії для всіх комп’ютерів учнів. Для цього на одній машині перевстановлюється все програмне забезпечення, виконуються відповідні налаштування, а потім на базі його створюється резервна копія системного розділу диску. На базі цієї копії може бути відновлена працездатність будь-якого комп’ютера учня.

Вторинна уніфікація. Якщо переустановлення програмного забезпечення повністю «з нуля» за якихось причин є неможливою, то проводиться створення резервної копії на кожному КУ(після відповідних підготовчих робіт: повної перевірки на віруси, дефрагментації і т.ін.). Цей спосіб вимагає збереження резервних копій залежно від кількості робочих місць.

Управління СІБ НКК та контроль за виконанням правил.

Системні утиліти, які забезпечують спостереження за роботою на КУ і керування КУ з комплекту вчителя (КВ), можуть бути використані як засоби централізованого управління безпекою. Вони дозволяють з одного комп’ютера виконувати більшість регламентних робіт СІБ (наприклад, запускати оновлення антивірусних баз, антивірусну перевірку жорстких дисків, перевірку програмного забезпечення (ПЗ) на цілісність і т. ін.).

Для чіткої організації робіт і підвищення надійності СІБ необхідно розробити і впровадити цілий ряд задокументованих процедур, які визначають обов’язки,

відповідальність персоналу при виконані регламентованих періодичних процедур, передбачити реакцію і дії у випадку інцидентів порушення правил безпеки та захисту НКК. Згідно визначення, інцидент – це будь-яке порушення правил інформаційної безпеки, встановлених в навчальному закладі. До інцидентів належать випадки програмно-апаратних збоїв та відмов, які викликані:

Несанкціонованими чи помилковими діями користувачів;

Проникненням вірусу у систему (чи іншого активного шкідливого коду);

Відмовою чи поломкою обладнання.

Для знаходження винуватця інциденту необхідно здійснювати протоколювання (аудит) критично важливих для КУ дій користувачів-учнів. Для прийняття обґрунтованого рішення про необхідну модифікацію СІБ НКК необхідно ввести роботи по виявлення частоти і видів даних інцидентів. Для цього у КІКТ повинно бути передбачено введення журналів обліку наступних форматів (див. таб.1 та таб.2)

Таблиця 1.

Журнал обліку програмно-апаратних збоїв та відмов.

Дата	№ комп'ютера	Опис проблем, що виникли	Дата виконання	Опис виконаних дій та причин проблеми

Журнал може заповнюватися вчителями, що проводять уроки в НКК, а виконуватися лаборантом чи іншими відповідальними особами, контроль за виконанням лежить на завідувачі лабораторією.

Таблиця 2.

Журнал самостійної роботи учнів в КІКТ.

Дата	Час початку роботи	№ комп'ютера	Які завдання виконувалися	Час закінчення роботи

Планування робіт з інформаційної безпеки за етапами життєвого циклу.

Поточне функціонування СІБ НКК неможливе без реалізації процедурних заходів, під якими розуміють усі періодичні регламентні роботи з інформаційної безпеки. Під час організації заходів з інформаційної безпеки, особливо важливим є планування та проведення комплексу взаємопов'язаних заходів на всіх етапах життєвого циклу СІБ НКК. Під *життєвим циклом* системи захисту інформації розуміються всі етапи її проектування, впровадження та експлуатації від початку створення до переходу на іншу програмно-апаратну платформу. Розподіл робіт за етапами життєвого циклу СІБ НКК показаний на мал.1. Оскільки життєвий цикл СІБ в основному збігається з життєвим циклом ІС, то більшість фахівців з інформаційної безпеки вважають, що найбільшої ефективності СІБ можна досягти лише за умови одночасної розробки ІС та її системи захисту. Потрібно врахувати вимоги 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 та сертифікації обладнання і програмного забезпечення. Розробка відповідної нормативної документації дозволить ввести СІБ УКК у всіх загальноосвітніх навчальних закладах та забезпечить вимогливе керівництво та сумлінне виконання на всіх рівнях – від директора до лаборанта.

З огляду на специфіку НКК як навчального середовища, доцільно базовим періодом проведення регламентних робіт періодом вважати навчальний рік. Це дозволяє всі організаційні та процедурні заходи планувати і проводити, узгоджуючи їх з особливостями навчального процесу та вимогами до його організації. Тому періодичними є процеси створення та оновлення резервних копій, знищення залишкових даних, оновлення бази облікових записів (видалення застарілих записів і створення нових), оптимізації роботи програмного забезпечення (ПЗ).

Планування регламентних робіт слід узгоджувати не лише з періодами навчального року, але і з навчальним планом і навантаженням на лабораторію. Тому доцільно під час календарного планування визначати не тільки дату, але і час, який є найбільш доцільним для проведення тих чи інших робіт. Деякі регламентні роботи рекомендується проводити в кінці робочого тижня, наприклад, планову антивірусну перевірку в п'ятницю перед кінцем робочого дня. Необхідною є також виділення відповідних годин на регламентні роботи в розкладі кабінету інформатики.

Завідувачем лабораторії кожен навчальний рік повинен розроблятися детальний календарний план регламентних робіт, в якому вказується дата і час їх проведення Регламентні роботи виконуються лаборантом і контролюються завідувачем. Вони складають основу безперервного циклу інформаційної безпеки НКК. Доцільним являється застосування програмних засобів, що автоматизують виконання планових завдань, зокрема, програм-планувальників (наприклад, Scheduled Tasks Explorer в Windows XP, Windows Server 2003)

Організаційні основи антивірусного захисту НКК.

Для ефективного захисту НКК необхідна не лише наявність антивірусного пакету на кожному комп'ютері, але й правильна організація роботи по антивірусному захисту.

До цього можемо включити такі пункти:

Обов'язкова наявність антивірусу-резидента в оперативній пам'яті.

Неможливість зміни налаштувань антивірусного захисту користувачами.

Обов'язкова перевірка всіх переносних носіїв.

Обов'язкове сканування і лікування всіх жорстких дисків.

Якнайчастіше встановлення оновлень ОС та антивірусних баз, що ліквідує знайдені уразливості.

Основними «входами» для шкідливого ПЗ, до якого належать віруси, черв'яки, трояни, є з'ємні носії та мережа Інтернет. Якщо взяти до уваги наявність локальної мережі, то будь-який вірус, проникнувши в мережу, буде розповсюджений по всіх робочих станціях. Для попередження зараження необхідно ввести строгі правила антивірусного захисту.

На кожній робочій станції НКК має бути встановлений антивірусний пакет, який проводить сканування на віруси в реальному часі. Всі системи, що підключені до мережі організації, повинні підлягати періодичній загальній перевірці, щоб виявляти заражені вірусами ОС та допоміжне програмне забезпечення. Перевірка на віруси жорстких дисків та оновлення антивірусних баз має проводиться з визначеним періодом.

На сервері Інтернету навчального закладу повинен бути встановлений антивірусний пакет, що проводить сканування вхідного трафіку на наявність вірусів та шпигунських програм. Виконання активного вмісту web-сторінок має бути обмежено. Завантаження будь-якого програмного забезпечення з Інтернету користувачам заборонено.

Навчальний заклад повинен проводити сканування кожного повідомлення електронної пошти на наявність вірусів, черв'яків і інших файлів, що виконуються, які становлять загрозу безпеці. Інфікована електронна пошта не повинна доставлятися користувачу.

Сторонні данні чи ПЗ повинні спочатку завантажуватися в ізольовану систему, на якій можна проводити опробування та тестування на наявність вірусів, помилок, закладок і інших проблем (наприклад проблем сумісності) при завантаженні цих даних чи встановленні цього ПЗ на інші системи в мережі.

Висновки

Ретельне планування і проведення регламентних робіт з інформаційної безпеки у загальноосвітніх навчальних закладах дозволить підвищити надійність функціонування програмної складової навчального комп'ютерного комплексу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гайкович В.Ю., Ершов Д.В. Основы безопасности информационных технологий. Учебное пособие/ Моск.гос.инженер.физ.ин-т(техн.ун.)– М.Изд-во МИФИ, 1995. – 93с.