НАЦІОНАЛЬНА АКАДЕМІЯ ПЕДАГОГІЧНИХ НАУК УКРАЇНИ
ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ЗАСОБІВ НАВЧАННЯ

В. М. Дем'яненко
В. Н. Ковальчук

Методичні рекомендації з інформаційної безпеки навчального комп'ютерного комплексу

Київ 2014

УДК 004.056:373.5
ББК 74.202:73

Затверджено на засіданні вченої ради Інституту інформаційних технологій і засобів навчання НАПН України, протокол № 9 від 25.09.2014 р.

Рецензенти:

Лапінський В.В. – кандидат фізико-математичних наук, доцент,
завідувач лабораторії навчання інформатики
Інституту педагогіки НАПН України.

Анікіна Л. – вчитель інформатики, вчитель вищої категорії, вчитель-методист

Методичні рекомендації з інформаційної безпеки навчального комп'ютерного комплексу / Укл. Дем'яненко В.М., Ковальчук В.Н. – К. : ІІТЗН НАПН України, 2014. – 39 с.

Проблеми інформаційних загроз для відкритого навчального середовища є дуже гострими в наш час. У методичних рекомендаціях розглянути комплекс питань, пов'язаних з інформаційною безпекою у середніх загальноосвітніх навчальних закладах. Окреслено основні проблеми інформаційної безпеки, методи та засоби захисту інформації та інформаційних ресурсів у навчальних комп'ютерних комплексах. Запропоновано методику створення та експлуатації типової системи захисту інформації, розраховану на практичне застосування в сучасних загальноосвітніх навчальних закладах.

Методичні рекомендації можуть бути корисними для педагогів та керівників навчальних закладів, які застосовують інформаційні технології у навчальному, для майбутніх та практикуючих учителів інформатики.

ЗМІСТ

1. Інформаційна безпека дітей в умовах загальноосвітнього навчального закладу.

1.1.Основні загрози для дітей та підлітків у сфері ІКТ.

Використання комп'ютерів у навчальному процесі є необхідною умовою сучасного навчання та виховання підростаючого покоління. Однак, в даному розділі, зосередимо свою увагу на негативних наслідках інформатизації та поширення інформаційних технологій у шкільних умовах. З усіх негативних впливів інформаційного середовища і можливих негативних наслідків впливу комп'ютерної техніки на дітей і підлітків ми виділимо ті, які підпадають під визначення інформаційної безпеки несформованої особистості.

Можемо сказати, що інформаційна безпека – це стан захищеності, тобто вона є властивістю системи мінімізувати інформаційні загрози. В першу чергу треба говорити про загрози, вони є первинними по відношенні до захисту від загроз. Для окремої особистості існують одні загрози, для суспільства інші, для держави – ще інші. Поширивши цю тезу вглиб, можемо вказати, що для дітей і молоді існують інші види загроз з огляду на вікові та психологічні особливості. Що для сформованої, зрілої особистості, не несе загрози, те для дитини може виявитися небезпечним. Несформованість психічної, вольової, емоційної сфери, недостатній рівень розвитку критичного мислення дітей і підлітків з одного боку, і часто вільний, неконтрольований доступ їх до джерел інформації, веде до підпадання їх під негативний інформаційний вплив, котрий може проявитися, як у деструктивних діях, так і в формуванні морально спотвореної особистості. Настільки людина сприйнятлива до психологічних впливів, загроз інформаційного середовища, наскільки в неї розвинені особистісні якості: психологічна стійкість, сила власних переконань, сила волі, критичне мислення. Однак, можна сказати, що несформована дитяча особистість, в силу її психічних особливостей, є найбільш уразливою до таких впливів.

Під *шкідливою* ми розуміємо інформацію, яка здатна негативно вплинути на особистість людини, її психіку, на прийняття нею рішень, загалом на поведінкові моделі та зміщувати ціннісно-орієнтаційні настанови в бік негативно оцінюваних у соціумі. Загалом шкідлива інформація, особливо у випадку дитини чи молодої людини, може нанести шкоду людині як цілісній особистості, що формується. Загроза шкідливої інформації, в основному, лежить не в площині фізичної шкоди, а в площині психологічного впливу на ціннісні орієнтири і самовизначення особистості у соціумі.

Отже, можемо дати визначення інформаційної безпеки особистості дитини. Основною відмінністю є те, що процес формування особистості у них ще не є закінченим, і саме вплив інформації, інформаційного середовища на формування даної особистості є в даній постановці питання вирішальним. Під інформаційною безпекою особистості, що формується, ми будемо розуміти, з одного боку, стан захищеності її життєво важливих інтересів, а з іншого – процес набуття особистістю таких якостей (вольових, інтелектуальних, емоційних), за наявності яких ніякі інформаційні впливи на неї неспроможні

викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху її стійкого прогресивного розвитку. Нове розуміння інформаційної безпеки вимагає переосмислення ролі освіти в процесі виховання нового покоління, здатного адекватно вписатися в новий інформаційний світ. Саме педагог, вчитель повинен стати основною ланкою у системі формування захисту молодої особистості від негативних інформаційних впливів. Потребують більш детальної розробки такі аспекти захисту особистості, що формується: правові, психологічні, педагогічні.

Зауважимо, що оскільки людина визначається найбільшою цінністю педагогіки гуманізму, то й інформаційно-психологічна безпека учнів є основною домінантою інформаційної безпеки особистості.

Розглянемо докладніше, які види загроз породжує новітній інформаційний простір для людини. Хоча найбільш серйозні небезпеки підстерігають наших дітей за межами моніторів, існує чимало серйозних ризиків, з якими діти зіштовхуються онлайн. Можемо сказати, що існує настільки великий спектр загроз для дітей і підлітків, що вони вимагають класифікації. Виходячи з аналізу [42], виділимо такі види загроз:

1) Загрози для особистісної безпеки
   - Загроза ознайомлення з матеріалами небажаного змісту(порнографія, ненормативна лексика, суіцидального характеру, сектантські, расистські та ненависницькі, вибухові речовини, хакерські сайти)
   - Загроза отримання недостовірної інформації
   - Загроза залежностей (комп’ютерної, ігрової, Інтернет і т.ін.)
   - Загроза спілкування з небезпечними людьми (шахраями, збоченцями , гриферами і т.ін)
   - Загрози вчинення протиправних дій (хакерство, порушення авторських прав і т.ін.)
2) Загрози витоку персональної інформації
   - Загроза розголошення конфіденційних даних (фамілії, імені, адреси, номерів кредитних карток, телефону і т.ін).
3) Загрози для персональних комп’ютерів
   - Загроза проникнення вірусів, черв’яків
   - Загроза завантаження шкідливого активного коду
   - Загроза завантаження програм з прихованими функціями: троянів, клавіатурних шпигунів і т.ін.

1.2.Основні методи попередження доступу учнів до небажаного змісту. Контент-фільтри.

1.2.1. Основні види небажаних Інтернет-ресурсів

Інтернет є могутнім інструментом навчання. Однак, окрім корисної інформації, учні можуть зустрітися з небажаним контентом. Наприклад, одержуючи доступ до невідповідної інформації на сайтах, присвячених злочинній діяльності або заходячи на сайти, що піддають ризикові їхню конфіденційність. Хоча нашу заклопотаність, у першу чергу, викликає

порнографічний і інший сексуальний контент, існують інші види неприйнятної доступної інформації, що може бути надзвичайно шкідливою для наших дітей. Останнє можна розділити на дві групи:

Заборонений контент для будь-якого віку та небажаний для дітей та підлітків. До ресурсів першого роду відносяться:

- Сайти з дитячою порнографією.
- Сайти терористів.
- Сайти, що розпалюють національну та расову ворожнечу.

До сайтів небажаних для дітей (крім вище згаданих) відносяться ті, які діти не повинні відвідувати за віковим обмеженням:

- Жорстокі ігри.
- Он-лайнові казино.
- Порнографія.
- Сайти, що пропагують насилля.
- Сайти сексуальних меншин.
- Сайти магазинів інтим-послуг.

Наявність у внутрішній мережі навчального закладу подібної інформації може викликати не лише претензії до учнів, які подібний контент скачують на робочу станцію мережі, але й карне переслідування адміністрації школи, яка допустила зберігання подібних матеріалів.

Відмітимо, що небажаним контентом може являтися також той, який відволікає дітей від учбового процесу. Діти можуть замість виконання навчального завдання в Мережі Інтернет, займатися переглядом дозволених матеріалів, але таких, що не мають безпосереднього відношення до учбового процесу.

1.2.2. Види контент фільтрації.

Проблема доступу дітей до небажаного змісту не може бути вирішена єдиним методом, а сукупністю програмних, виховних та організаційних заходів. Розглянемо основні з них:

Контент-фільтр – це система, що блокує доступ до небажаних ресурсів Інтернету, виходячи з тих або інших критеріїв. Контент фільтри можуть бути реалізовані в різних програмних комплексів або як самостійний програмний продукт. Наприклад, в складі мережних екранів чи проксі-серверів. Мережні екрани призначені для обмеження доступу між різними мережами, вони перевіряють весь трафік, що минає їх, і блокують заборонений.

Обрані сайти – заздалегідь строго визначається сукупність сайтів, до яких буде дозволений доступ дітей. Найчастіше використовується при неможливості прямого доступу НКК до мережі Інтернет.

Дитячі пошукові машини – це такі, що створені на базі існуючих пошукових машин спеціально для школярів і здійснюють фільтрацію посилань, що видаються користувачеві виходячи з вікових обмежень.

На базі Google вчителі можуть створювати свої власні тематичні пошукові машини для того, щоб школярі, не "перелопачували" весь Інтернет у пошуку

необхідної інформації. Будь-які користувачі, зареєстровані в офісі Google колективно редагувати і поліпшувати ці пошукові машини.

У такий спосіб може бути вирішена проблема захисту школярів від нерелевантної інформації, яку вони можуть одержати, направляючи запити в пошукові машини "загального користування".

Інші методи захисту неповнолітніх користувачів.

Спостереження за використанням чатів. Використання чату в навчальних цілях завжди повинне проводитися під спостереженням учителя.

Спеціально набудована система електронної пошти. Це поштовий сервер шкільного призначення з налаштованими обмеженнями щодо того, кому і як можна відправляти електронні повідомлення. Школи можуть обмежити поштовий зв'язок тільки внутрішніми користувачами, а зовнішній дозволяти винятково через учителя. Деяким учням може бути дозволено, посилати пошту на зовнішні адреси, але тільки за заздалегідь визначеним їх списком.

Використання систем спостереження. Для моніторингу найкраще використовувати програми, які дозволяють спостерігати за діями учнів з учительського комп'ютера. Обов'язковим є ведення журналів, що протоколюють дії дітей в Інтернеті.

1.2.3. Проблема проникнення/витоку контенту з навчального закладу. Трафікоємні процедури

Дотепер ми говорили про те, що в навчальному закладі є проблема проникнення небажаного контенту усередину навчальної мережі. Але існує також проблема витоку контенту. У даному випадку, по-перше, мова йде про витік приватних персональних даних. У сучасному суспільстві існує проблема викрадення дітей, сексуальні домагання і ін. Тому особиста інформація про дитину (її фотографія, розклад уроків, e-mail, телефон) не повинні вивішуватися в Мережі для вільного доступу.

При розміщенні фотографій у Мережі (наприклад, на шкільному Web-сайті) бажано розміщати фотографії дітей тільки за згодою батьків або тільки групові. Не варто вказувати імена дітей і іншу особисту інформацію.

Друга проблема – це розсилання поштою або розміщення на шкільному (або іншому) сайті забороненого контенту. Розсилання піратського ПО, порнографії і т.п.

Небажаний контент потрапляє в мережу навчального закладу переважно по двох каналах: через Web-трафік і через поштовий трафік.

Проблема фільтрації поштового трафіку широко відома як проблема спаму. У якості спама можуть поширюватися повідомлення образливого характеру, заклики до насильства і т.п. Крім усіх перерахованих вище проблем, спам до того ж генерує зайвий трафік, відволікає користувачів.

Звичайно, важливим є запобігання розповсюдженню та вилучення подібного контенту з flash-нагромаджувачів, CD, DVD дисків та жорстких дисків НКК.

Трафікоємні процедури – скачування відеофільмів, музики, файлових архівів програмного забезпечення ведуть до різкого збільшення трафіку, що може сповільнювати роботу мережі і збільшувати витрати на оплату трафіку. Більшість програм, що блокують доступ до заборонених Web-сайтів, забезпечують і контроль трафікоємних процедур.

Насамперед , варто сказати, що проблема захисту від шкідливого контенту далеко не тільки шкільна проблема. Використання інтернету співробітниками або учнями, не зв'язане з навчальною або службовою діяльністю, одержало назву "киберслэкинг" (від англ. cyberslacking - дослівно на російській "кибербездельничание").

Навчальні заклади аж ніяк не першими стали намагатися вирішити проблему фільтрації Інтернету. Це, з одного боку, говорить про те, що проблема глобальна і просто не вирішується, а з іншої, що навчальним закладам у ряді випадків можуть підійти рішення, створені для організацій широкого профілю. Відзначимо також, що віруси, трояни, шпигунські програми й інші шкідливі коди теж можуть легко передаватися через Web.

1.2.4. Боротьба з небажаним контентом.

У боротьбі можна виділити організаційні заходи (призначення відповідальних осіб, створення режиму доступу в комп'ютерний клас, доведення до відома учнів норм поводження у Мережі, відповідальності за протиправні дії і т.п.) і технічні. До технічних заходів відносяться фільтрація трафіку і моніторинг дій учнів.

Наявність моніторингу (навіть без фільтрації) уже може стати ефективним заходом. Якщо учень буде знати, що за його діями (усіма відвідуваннями ведеться постійний моніторинг і всі його дії записуються в log-файлах із вказівкою того, хто, коли і що відвідував), то це вже в істотній мері обмежить імовірність відвідування небажаних сайтів.

Варіанти фільтрації контенту.

Контент може фільтруватися на рівні провайдеру, на рівні шлюзу в Інтернет мережі, що захищається, і на рівні клієнтської станції.

Фільтрація може бути побудована на основі зовнішньої оновлюваної бази даних заборонених ресурсів і може бути побудована на основі локальної програми, що діє по власних принципах фільтрації ("чорні", "білі" списки, ключові слова і т.п.).

При цьому в принципі фільтрація може бути побудована за принципом:

1. "Забороняємо все, крім того, що можна" 2. "Можна все, крім того, що заборонено"

Звичайно, реалізувати фільтрацію за принципом "Забороняємо все, крім того, що можна", побудувати досить просто, подібна форма, можливо, має сенс для молодших школярів, але в цьому випадку Інтернет утрачає багато своїх функцій.

Другий варіант вимагає побудови і постійного оновлення величезної бази даних (підтримувати її повинен провайдер сервісу), що постійно поповнює базу забороненого контенту.

Для повноцінної реалізації другого виду фільтрації необхідно проіндексувати мільярди Web-сторінок, і це під силу тільки великим провайдерам подібного сервісу, наприклад, таким як iSS, Proventia Web Filter. Чим більше база, тим якісніше і дорожче рішення.

Складності фільтрації контенту в школах.

Щодня в Інтернеті з'являються тисячі нових сайтів, тому, навіть використовуючи відновлення баз даних з небажаними ресурсами, домогтися 100%-ної фільтрації неможливо. Окрема проблема - це недостатня фільтрація російськомовного та україномовного контенту західними продуктами. Можливі помилки, коли фільтр буде відсівати сайти корисного змісту. Загалом, чим більш інтелектуальний фільтр і чим більша база, на яку він спирається, тим дорожче рішення і тим воно менш доступне для шкіл.

Часто в школах встановлено різне комп'ютерне устаткування і програмні продукти фільтрації контенту (Web і e-mail), що працюють на різних платформах. Адміністратори в школах мають різний досвід роботи з комп'ютерами, і навіть непрофесіонал повинен мати можливість створювати і підтримувати політику фільтрації. Освітній процес включає безліч різних областей науки, і фільтрація повинна бути всеосяжною, що набудовується, а також забезпечувати захист від новітніх погроз.

Моніторинг Інтернет активності.

Моніторинг і протоколювання - це в багатьох випадках перший і найважливіший крок у контролюванні Інтернет доступу. Дана функція наочно показує серфінг-профіль користувача. Учитель може перевірити, де знаходився учень, що переглядав, у який час і як довго. Моніторинг дає швидку і точну картину Web серфінгу. Дані про Інтернет-активність захищені криптографічно і зберігаються в недоступному для неавторизованого перегляду вигляді. Будь-який відвіданий ресурс може бути переглянутий, і згодом доданий у список дозволених або заборонених сайтів. Звіти моніторингу (Monitoring Reports) чітко показують, які Web-сторінки відвідувалися, час візиту, Web-адресу, і іншу інформацію.

1.3.Комплекс заходів для захисту учнів від загроз ІКТ

1.3.1. Організаційні, програмно-апаратні та виховні заходи. Правила інформаційної безпеки для учнів

Політика інформаційної безпеки по відношенню до користувачів-учнів повинна бути вироблена у кожному навчальному закладі і конкретизована у вигляді правил з ІБ (див. Додаток С). Вкажемо, що основними *принципами політики безпеки* повинні бути: послідовність, обов’язковість, карність.

Необхідні заходи захисту НКК від навмисних та ненавмисних дій учнів: контроль з боку вчителя, персоналізація та обмеження доступу до критичних ресурсів, контроль і реагування на НСД програмних засобів захисту, реагування персоналу, вчителя і застосування відповідних виховних заходів.

Основна мета політики безпеки НКК – це забезпечення виконання учнями-користувачами правил інформаційної безпеки, які унеможливлюють чи зводять до мінімуму шкоду, яку вони можуть спричинити своїми діями, навмисними чи

ненавмисними, програмному компоненту НКК. Ця мета реалізується організаційними, програмно-апаратними та виховними заходами.

Комплексний підхід до інформаційної безпеки вимагає поєднання таких заходів по відношенню до користувачів-учнів: контроль з боку вчителя (перш за все візуальний), контроль і реагування на несанкціоновані дії (НСД) програмних засобів захисту, реагування персоналу, вчителя при виникненні НДС і застосування відповідних виховних заходів. Під несанкціонованими, ми будемо розуміти дії, що заборонені політикою безпеки і конкретизовані у правилах користувачів.

До **організаційних** заходів належать перш за все розробка, впровадження та контроль за виконанням політики безпеки СІБ НКК по відношенню до користувачів-учнів. Контроль за виконанням покладено на вчителів та обслуговуючий персонал.

Особливої уваги потребує проблема доступу дітей до Інтернету.

Правила щодо доступу в Інтернет, встановлені в школі, повинні бути формалізовані, тобто мати вигляд обов'язкового документа. Відповідно до світового досвіду, можливою формою цього документу є підписана учнями, їхніми батьками і вчителями письмова угода, що визначає порядок використання Інтернету - тобто формалізовані правила для Мережі набувають рис "колективного договору". Ці правила повинні обов’язково включати інструкцію з публікації в Інтернету особистих даних учнів, їхніх фотографій, аудіо- і відеоматеріалів і тощо.

Частина правил політики безпеки, що стосується доступу учнів до Інтернету, повинна бути повідомлена перед початком відповідних занять. Найкращий варіант - коли учитель виконує роль не доглядача, а консультанта. Цього можна спробувати досягти, провівши бесіду з дітьми, де їм буде докладно розказано про небезпеки, що існують в Інтернеті, необхідно навчити їх правильно виходити з неприємних ситуацій. Інструкції з безпечного використання Інтернету повинні бути роз'яснені учнем до того, як вони одержать доступ до Інтернету або їм нададуть індивідуальні адреси електронної пошти. На закінчення бесіди поясніть обмеження на використання Інтернету й обговоріть їх з дітьми. Спільно збільшити безпеку використання Мережі набагато простіше.

Програмно-апаратні засоби прийнятої політики безпеки реалізуються через систему управління (контролю) доступу користувачів до ресурсів, яка включає ідентифікацію та автентифікацію користувачів, управління (контроль) доступу до ресурсів, протоколювання та аудит дій користувачів. Програмно-апаратні засоби повинні гарантувати захищеність критично важливих компонентів ПЗ НКК від несанкціонованих і помилкових дій користувачів. В правилах розмежування доступу необхідно заборонити доступ цих користувачів до системних областей диску, а також заборонити модифікацію ними програмного забезпечення, навчальної та іншої важливої інформації. Рекомендується забезпечити доступ в Інтернет тільки з тих комп'ютерів, що постійно знаходяться в полі зору вчителя. Також варто використовувати

програми, що дають можливість відображати вміст екранів усіх комп'ютерів на моніторі вчителя і тим самим дозволяють стежити за діяльністю учнів.

Основними в реалізації політики безпеки НКК є *виховні* заходи. Оскільки вони використовуються як для попередження НСД, так і для впливу на порушників правил безпеки з метою їх перевиховання. Дуже важливо встановити правила покарання тих, хто зловживає доступом; порушення можуть бути і не настільки значними, але повинні бути обговорені, а за серйозні провини повинні бути передбачені серйозні заходи покарання.

Не слід забувати, що основним завданням школи є виховання майбутнього громадянина. З кожним роком зростає кількість працівників, які тим чи іншим чином використовують у своїй повсякденній роботі інформаційні технології. Також, безсумнівно, зростає роль інформаційної безпеки як неодмінної складової будь-якої інформаційної системи. Найуразливішою ланкою будь-якої системи безпеки були і будуть люди. Тому майбутнього кваліфікованого працівника неможливо уявити без необхідних базових знань з інформаційної безпеки. Важливу роль тут грає не лише навчання, але й виховання, оскільки лише воно забезпечує засвоєння морально-етичних норм в галузі інформаційних технологій.

Політика безпеки роботи з користувачами-учнями, з педагогічної точки зору, повинна сприяти вихованню учнів, зокрема преміювати (розширювати права) за хорошу поведінку і «карати» за погану. Основні методи, які використовують для безумовного виконання політики безпеки користувачами є інформування, контроль, спонукання, попередження, тимчасова заборона (відмова в доступі), зменшення наданих прав і привілеїв (як користувача НКК) та інші.

Головна мета виховних заходів є усвідомлення учнями відповідальності за свої дії навіть у «віртуальному» середовищі, засвоєння етичних норм поводження в цьому середовищі, результатом чого є формування в учнів компетентності з інформаційної безпеки.

1.3.2. Питання інформаційної безпеки в шкільному курсі інформатики.

В шкільному курсі інформатики є достатньо резервів для внесення основних питань інформаційної безпеки до змісту навчального курсу основи інформатики. Так, пропонується доповнити шкільний курс такими питаннями:

1) Інформація в Інтернет: чи завжди вона є правдивою?
2) Поняття про загрози. Загрози для особистості в Інтернеті.
3) Поняття про кіберзалежності і їх основні ознаки.
4) Основні закони в сфері захисту інформації.
5) Основні поняття про захист інформації, захист персональних даних. Права власності в Інтернеті.
6) Основні правила етичного спілкування в Інтернеті. Питання комп’ютерної етики.
7) Основи безпечної роботи в мережі Інтернет. Поняття про між- мережний екран та захист ПК.

1.3.3. Просвіта батьків з питань інформаційної безпеки

Враховуючи розширення змісту діяльності вчителя інформатики, необхідності розвитку його компетентності, що стосується наданням інформаційно-консультаційних послуг учителям, батькам, учням, а також широкого розповсюдження домашніх ПК, слід розвивати їхнє уміння переконувати батьків у необхідності захисту дітей від шкідливої інформації. З відомостями про небезпеки онлайнового середовища необхідно ознайомити не лише учнів, але й батьків. До того ж одним з основних завдань вчителя інформатики є потреба навчити дітей і підлітків уникати небезпек Мережі. Як утримати учнів від доступу до веб-сайтів, що містить непристойні матеріали, і від контакту з особами, що представляють для них загрозу? Щоб захистити учнів і переконати в необхідності цього їхніх батьків, необхідно прийняти заходи, спрямовані на запобігання будь-яких несанкціонованих вторгнень в інформаційний простір школи. Варто одержати згоду батьків на прийняття рішень, що можуть викликати ризик для дітей, і спробувати зробити їх учасниками прийняття рішень. Для цього учителі повинні розповісти батькам, у яких цілях вони використовують Інтернет у школі, які можуть бути небезпеки і як вони контролюють ризики. Повідомлення повинне бути ясним і чітким (закінченим), і викладати усю важливу інформацію так, що навіть самий необізнаний у комп'ютерному відношенні батько міг би її зрозуміти.

Необхідність консультації батьків про можливості програмного забезпечення і технічної реалізації, не допущення доступу дітей до шкідливої інформації через домашнє ПК вимагає отримання майбутніми вчителями компетенції з питань інформаційної безпеки.

1.3.4. Рекомендації по захисту дітей від доступу до інформації, що не сумісна з завданнями навчання

Знаходячись в комп'ютерному класі з групою учнів, що досліджують Інтернет, - непроста задача. У Вас виникають сумніви, чи проводять вони свій час з користю або дарма його витрачають? От деякі дії, що може почати вчитель, щоб збільшити безпеку учнів в Інтернеті.

1) Розберіться в основних питаннях безпеки Інтернету, перш ніж ввійти в клас.
2) Упевніться, що Ви, по можливості, інформовані про ті функції, що виконують шкільні комп'ютери.
3) Довідайтеся, чи встановлені на шкільних комп'ютерах фільтри або програмне забезпечення для захисту дітей; якщо встановлені, з'ясуєте, яке саме.
4) На початку уроку, коли комп'ютери ще не включені, обговоріть з дітьми, що можна чекати від дослідження Інтернету.
5) Нагадайте учням про техніку безпеки і правила користування Інтернетуом.
6) Не дозволяйте учням блукати по Мережі - вони можуть потрапити в небезпечну зону; виберіть декілька сайтів, що викликають інтерес, і зосередьте на них увагу дітей.

7) Стежте за тими учням, що швидко виключають монітори, сміючись над побаченим на екрані, групуються навколо одного комп'ютера або виглядають збентеженими - це попереджувальні знаки потенційної неприємності.
8) Винагородіть тих учнів, що поводяться відповідально в Інтернеті; зробіть їх прикладом наслідування для іншої частини класу.
9) Замість того щоб забороняти улюблені заняття учнів в Інтернеті (чати, електронна переписка), досліджуйте можливості використання цих технологій для розширення навчання й одержання знань.[44]

2. Організаційні та процедурні заходи з інформаційної безпеки. Програмно-апаратні засоби

2.1. Організація роботи кабінету інформатики з урахуванням заходів з інформаційної безпеки.

Окремо взяті технічні чи програмні засоби не можуть діяти без організованої і 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 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». [12, с.31] Оскільки, на даному етапі інформатизації загальноосвітніх навчальних закладів є труднощі з виділенням коштів на закупівлю чи оновлення саме програмно-апаратних засобів, то для захисту НКК можемо використовувати лише наявні їх можливості. Тому найбільш перспективним вбачається максимальне використання організаційних та виховних заходів для підвищення ефективності СІБ НКК, впровадження яких не вимагає витрати додаткових коштів. Саме комплексний підхід до інформаційної безпеки НКК, усвідомлення необхідності таких заходів на всіх рівнях управління освітою, навчанням та підвищенням компетентності обслуговуючого персоналу та вчителів інформатики, є запорукою успішної реалізації вимог висунутих до надійності програмної складової НКК.

2.1.1. Методи оптимізації і підвищення надійності роботи КІІТК.

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 цих 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 ПЗ НКК.

Серед основних методів, що використовуються для підвищення захищеності і відновлюваності програмної складової інформаційної системи (ІС), є резервування та періодична перевірка його цілісності. Ці методи можуть реалізовуватися системними утилітами, що 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 пошкодження достатньо значні чи зачіпають критично важливі файли операційної системи, то для їх відновлення необхідно мати резервну копію системної області жорсткого диску. Системні утиліти, що створюють архіви-образи логічних дисків допомагають швидко відновити роботу пошкодженої операційної системи не перевстановлюючи її. Необхідною умовою використання цих засобів є чітке планування і виконання регламентних робіт персоналом. Наприклад, образ системного диску обов'язково робиться, як мінімум раз на навчальний рік після відповідних підготовчих робіт, а перевірка файлів на цілісність має проводитися за визначеним періодом.

Резервування.

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 КУ) вирішується проведенням уніфікації. Див. далі.

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

йього 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.

2.1.2. Управління СІБ НКК та контроль за виконанням правил.

Системні утиліти, які забезпечують спостереження за роботою на комплекті учня (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.). Деякі програми містять внутрішній планувальник або ж можна скористатися планувальником операційної системи (ОС) для запуску програм СІБ, що економить час обслуговуючого персоналу.

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, перетбачити реакцію і дії у випадку інцидентів порушення правил безпеки та захисту НКК. Згідно визначення, інцидент – це будь-яке порушення правил інформаційної безпеки, всановлених в навчальному закладі. До таких інцидентів належать:

- Програмно-апаратний збій чи відмова, які викликані:
- Несанкціонованими чи помилковими діями користувачів;
- Проникненням вірусу у систему (чи інших АШК);
- Відмовою чи поломкою обладнання.
- Протоколювання, виявлення частоти і видів даних інцидентів.

Останній пункт необхідний, для прийняття обґрунтованого рішення про необхідну модифікацію СІБ НКК.

Документи (журнали обліку). Всі документи можуть вестися як електронному, так і в паперовому вигляді.

Журнал обліку програмно-апаратних збоїв та відмов.

Форма №1.

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 зав.лабораторією.

Журнал самостійної роботи учнів в КІІКТ.
Форма №2.

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

2.1.3. 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.

При організації антивірусного захисту необхідно передбачити періодичність і дати антивірусної перевірки та оновлення баз. Автоматизація цього процесу вимагає залучення програми-планувальника (наприклад, Scheduled Tasks Explorer в Windows XP, Windows Server 2003) для перевірок. Періодичність антивірусних заходів встановлюється календарним планом регламентних робіт, що є обов'язковим для виконання.

При виборі та налаштуванні програмного антивірусного комплексу для НКК, корисно брати до уваги такі міркування.

- Можливості оновлення антивірусних баз: частоту, простоту встановлення і можливість оновлення по мережі.
- Вимогливість до системних ресурсів.
- Можливості віддаленого керування та сканування по мережі.
- Наявність вбудованого планувальника.
- Надійність у роботі і простота експлуатації.
- Необхідність обов'язкової перевірки з'ємних носіїв.

Якщо ми розглянемо мал. 2 (с.25), то побачимо, що основними «входами» для шкідливого ПЗ, до якого належать віруси, черв'яки, трояни, є з'ємні носії та мережа Інтернет. Якщо з 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.

Обов’язок користувачів полягає у сприянні заходам антивірусного захисту. Користувачі повинні перевіряти всі дані при кожному їх завантаженні з будь-якого джерела. Також необхідно перевіряти будь-який з’ємний носій перед його відкриттям на наявність вірусів. Користувачі повинні сприяти оновленню антивірусних баз, а також ніколи не перешкоджати та не вивантажувати з оперативної пам’яті антивірусні програми.

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.

2.2. Програмно-апаратні засоби захисту КІІКТ.

Переходячи до програмно-апаратного рівня реалізації системи захисту НКК, ми розглянемо основні напрямки його захисту і особливості програмного забезпечення, які ці функції реалізують.

«Найбільш значимими для захисту автоматизованих систем є програмні засоби захисту, що дозволяють створювати модель захищеної автоматизованої системи з побудовою правил розмежування доступу, централізовано управляти процесами захисту, інтегрувати різні механізми і засоби захисту в єдину систему».[30, с.10].

Однак саме програмна частина ННК є найбільш уразливою до помилкових дій великої кількості недосвідчених користувачів і саме вона, поряд з апаратною, створює передумови безперебійної роботи всього комплексу. Тобто, об’єктом захисту виступає не стільки інформація, в класичному розумінні інформаційної безпеки, скільки асоційовані з нею інформаційні ресурси.

2.2.1. Аналіз наявного програмно-апаратного забезпечення.

Виходячи з нормативних документів, а також реалій сьогодення, можемо зазначити, що програмне забезпечення НКК є недостатнім для реалізації СІБ у повному обсязі. До того ж в багатьох школах є застарілим не лише обладнання, а й програмне забезпечення. Тому, розробляючи алгоритм створення СІБ НКК, будемо враховувати значну різницю в програмному забезпеченні, а також неможливість його негайного оновлення.

Проведений аналіз наявного у школах ПЗ дає можливість виділити такі його класи:

- Windows 95/98/Me
- Windows 2000/ XP

Наприклад, ось що говорить Крисін А.В. [19, с.38], порівнюючи цих два класи. «Не секрет, що в Windows 2000/ NT/XP існує ціла система безпеки, яка дозволяє захистити ваш комп'ютер майже від будь-якої несанкціонованої дії. На жаль, багато користувачів вимушені працювати під Windows 95/98/Me, які є абсолютно беззахисні. Особливо страждають від цього комп'ютери в учбових закладах, доступ до яких зовсім не обмежений».

Щодо лінійки Windows, то з кожною версією вбудовані засоби захисту і безпечність ОС зростають. Ми надалі будемо орієнтуватися на однорангову мережу, побудовану на базі Windows XP Pro, оскільки такі вимоги не тільки зазначені в нормативних документах, але й є найбільш розповсюдженими у даний час.

При побудові СІБ, ми повинні, в основному, спиратися на можливості ОС, то для кожного варіанту опишемо відповідну **стратегію** захисту. Стратегія захисту складається з стратегії адміністрування користувачів (яка залежить від можливостей ОС) та програмно-апаратних засобів захисту.

Для цього опишемо більш детально стратегію безпеки Windows 2000/XP, використавши матеріали з книжки Крисіна А.В. [19, с.56-65].

Модель безпеки Windows 2000/XP заснована на поняттях аутентифікації й авторизації. У Windows 2000/XP також існують технології шифрування, що захищають конфіденційні дані на диску й у мережі:наприклад. EFS (Encrypting File System) - технологія відкритого ключа.

2.2.2. Windows XP. Аутентифікація.

Реєструючи на комп'ютері для одержання доступу до ресурсів локального комп'ютера або мережі, користувач повинен увести своє ім'я і пароль. У Windows 2000/XP можлива єдина реєстрація для доступу до всіх мережних ресурсів. Таким чином, користувач може ввійти в систему з клієнтського комп'ютера по єдиному паролі або смарт-карті й одержати доступ до інших комп'ютерів домену без повторного введення ідентифікаційних даних.

Головний протокол безпеки в доменах Windows 2000 – Kerberos 5. Для аутентифікації на серверах під керуванням Windows NT 4.0 і доступу до ресурсів доменів Windows NT, клієнти Windows 2000/XP використовують протокол NTLM. Комп'ютери з Windows 2000/XP, що не належать до домену, також застосовують для аутентификации протокол NTLM.

Використовуючи Windows 2000/XP у мережі з активним каталогом (Active Directory), можна керувати безпекою реєстрації за допомогою параметрів політики груп, наприклад, обмежувати доступ до комп'ютерів і примусово закінчувати сеанси роботи користувачів через заданий час. Можна застосовувати попередньо сконфігуровані шаблони безпеки, що відповідають вимогам безпеки даної робочої станції або мережі. Шаблони являють собою файли з попередньо сконфігурованими параметрами безпеки, які можна застосовувати на локальному комп'ютері або імпортувати у групові політики активного каталогу. Ці шаблони використовуються в незмінному виді або налаштовуються для визначених уразливостей.

2.2.3. Windows XP. Авторизація.

Авторизація дозволяє контролювати доступ користувачів до ресурсів. Застосування списків керування доступом (access control list, ACL) і прав доступу NTFS гарантує, що користувач одержить доступ тільки до потрібних йому ресурсів, наприклад, до файлів, дисків (у тому числі мережних), принтерів і додатків. За допомогою груп безпеки, прав користувачів і прав доступу можна одночасно керувати безпекою як на рівні ресурсів, так і на рівні файлів, папок і прав окремих користувачів.

2.2.4. Windows XP. Групи безпеки.

Групи безпеки спрощують керування доступом до ресурсів. Можна приписувати користувачів до груп безпеки, а потім надавати цим групам права доступу. Можна додавати користувачів до груп безпеки і видаляти їх звідти відповідно до потреб цих користувачів.

Оснащення MMC Computer Management дозволяє створювати облікові записи користувачів і поміщати їх у локальні групи безпеки. Можна надавати користувачам права доступу до файлів і папок і визначати дії, що користувачі можуть виконувати над ними. Можна дозволити і спадкування прав доступу. При цьому права доступу, визначені для каталогу, застосовуються до всіх його підкаталогів і файлів, що знаходиться в них.

Серед груп безпеки, локальних для домену і комп'ютера, існує ряд попередньо сконфігурованих груп, у які можна включати користувачів :

Адміністратори (Administrators) мають повний контроль над локальним комп'ютером і правами на здійснення будь-яких дій. При установці Windows 2000/XP для цієї групи створюється і призначається убудований обліковий запис Адміністратор (Administrator). Коли комп'ютер приєднується до домену, за замовчуванням до групи Адміністратори додається група Адміністратори домену (Domain Administrators).

Досвідчені користувачі (Power Users) мають права на читання і запис файлів не тільки в особистих папках, але і за їхніми межами. Вони можуть установлювати додатки і виконувати багато адміністративних дій.

Користувачі (Users) у відношенні до більшої частини системи мають тільки право на читання. У них є право на читання і запис тільки файлів їх особистих папок. Користувачі не можуть читати дані інших користувачів (якщо вони не знаходяться в загальній папці), установлювати додатка, що вимагають модифікації системних каталогів або реєстру, і виконувати адміністративні дії.

Гості (Guests) можуть реєструватися по убудованому обліковому записі Guest і виконувати обмежений набір дій, у тому числі виключати комп'ютер. Користувачі, що не мають облікового запису на цьому комп'ютері, або користувачі, чиї облікові записи відключені (але не вилучені), можуть зареєструватися на комп'ютері по обліковому записі Guest. Можна встановлювати права доступу для цього облікового запису, що за замовчуванням входить в убудовану групу Guests. За замовчуванням обліковий запис Guest відключений.

Можна сконфігурувати списки керування доступом для груп ресурсів або груп безпеки і в міру необхідності додавати/видаляти з них користувачів або ресурси, що полегшує керування правами доступу і їхній аудит. Можна надати користувачам права на доступ до файлів і папок і вказати дії, які можна виконувати з ними. Можна також дозволити спадкування прав доступу; при цьому вказані права до деякої папки застосовуються і до її підкаталогів і файлів, що знаходиться в них.

2.2.5. Windows XP. Політика груп.

Параметри політики груп дозволяють призначати ресурсам права доступу, а також надавати права доступу користувачам. Це потрібно для того, щоб вимагати запуску визначених додатків тільки в заданому контексті безпеки (тим самим знижуючи ризик впливу на комп'ютер небажаних додатків, наприклад, вірусів) і конфігурувати різні права доступу для безлічі клієнтських комп'ютерів. Можна зконфігурувати права доступу на еталонному комп'ютері, що буде використаний як базовий образ для установки цих прав на інші робочі станції, гарантуючи, таким чином, стандартизоване керування безпекою навіть під час відсутності Active Directory.

Функції аудита дозволяють виявляти спроби відключити або обійти захист ресурсів. Можна задіяти попередньо сконфігуровані шаблони безпеки, що відповідають вимогам безпеки для даної робочої станції або мережі. Шаблони безпеки - це файли з попередньо встановленими параметрами безпеки, що застосовують до локального комп'ютера або імпортують у групові політики активного каталогу (Active Directory). Шаблони безпеки використовуються в незмінному виді або набудовуються у відповідності з визначеними завданнями.

2.2.6. Windows XP. Шифрування.

Шифрована файлова система (EFS) дозволяє користувачам зашифрувати і розшифровувати файли. EFS використовується для захисту файлів користувачів від зловмисників, що можуть одержати несанкціонований фізичний доступ до збережених конфіденційних даних (наприклад, викравши переносної комп'ютер або зовнішній диск).

Користувачі працюють із зашифрованими файлами і папками так само, як і з іншими файлами і папками. Шифрування прозоре. Якщо користувач EFS є особою, що зашифрувала файл або папку, система автоматично розшифровує їх при наступному доступі. Однак для зловмисників зашифровані файли і папки недоступні.

Шифрована файлова система (EFS) забезпечує ядро технології шифрування файлів, що використовуються для збереження шифрованих файлів на томах файлової системи NTFS. Після того як файл або папка зашифровані, з ними працюють так само, як і з іншими файлами або папками. Шифрування є прозорим для користувача, що зашифрував файл. Це означає, що перед використанням файл не потрібно розшифровувати. Файл можна відкрити і змінювати, як це робиться звичайно. Однак зловмисникові, що намагається одержати доступ до зашифрованих файлів або папок, не зможе це зробити.

Зловмисник одержить повідомлення про відмовлення в доступі, якщо він спробує відкрити, скопіювати, перемістити або перейменувати зашифрований файл або папку.

Шифрування і розшифровування файлів виконується установкою властивостей шифрування для папок і файлів, як встановлюються й інші атрибути, наприклад, "тільки читання", "стиснутий" або "схований". Якщо шифрується папка, усі файли і підпапки, створені в зашифрованій папці, автоматично шифруються. Рекомендується використовувати шифрування на рівні папки. Файли і папки можуть також бути зашифровані або розшифровані з допомогою функції командного рядка cipher.

2.2.7. Windows XP. Рекомендації з використання EFS.

Зашифруйте папку "Мої документи", тому що в ній автоматично зберігається більшість документів. Це гарантує шифрування особистих документів за замовчуванням.

Зашифруйте папку Temp, щоб будь-які тимчасові файли, створювані програмами, шифрувалися автоматично. Шифруйте папки замість окремих файлів, щоб тимчасові файли, що створюються програмами-додатками в процесі редагування, також були зашифровані.

За допомогою команди Експорт з об'єкта MMC "Сертифікати", зробіть на гнучкому диску резервні копії сертифіката шифрування файлів і пов’язаного з ним закритого ключа. Зберігаєте гнучкий диск у безпечному місці. Якщо сертифікат шифрування файлів буде загублений (через збій диска або по якій-небудь іншій причині), за допомогою команди імпорт з об'єкта MMC "Сертифікати" сертифікат і пов'язаний з ним закритий ключ можуть бути відновлені з гнучкого диска, а зашифровані файли - відкриті.

2.3.Безпека Інтернету.

Очевидно, що можливість виходу у глобальну мережу є важливим і необхідним чинником підвищення ефективності навчального процесу для кожного навчального закладу. Однак, не слід забувати, що це нововведення несе низку загроз.

Зауважимо, що на даний час приблизно 70% шкільних комп’ютерних класів підключенні до Інтернету. Найчастіше це є Dial-Up з’єднання за допомогою телефонної лінії. Таке з’єднання, як правило, використовується для виходу в Інтернет з одного (учительського) комп’ютера. Всі проблеми аналогічні з тими, що виникають при підключення до Інтернету одиничного персонального комп’ютера.

Однак технології не стоять на місці. Тому кількість шкіл для яких є технічно можливою організація колективного доступу до Інтернету, з кожним роком збільшується. Проблеми безпечного колективного доступу до Інтернету ми розглянемо другій частині даного розділу.

Розглянемо основні з них.

Проблема 1. Можливість розголошення даних користувача.

Проблема 2. Вона стосується, на нашу думку, підключення до Інтернету НКК. Робить освітню локальну мережу більш уразливою до віддалених атак, а також є додатковим джерелом проникнення шкідливих програм.

Освітні мережі цілком можуть стати об'єктом ненаправлених атак (наприклад, хакерських), хоча і не завжди містять цінну інформацію. Останнім часом спостерігається тенденція на проведення атак, які захоплюють контроль над віддаленою системою, перетворюючи її на «зомбі». Тобто, можливість використання ресурсів «захопленої» системи є достатнім стимулом для проведення атак хакерами.

Також при доступі неповнолітніх до Інтернету слід враховувати необхідність їхнього захисту від аморальної та іншої шкідливої інформації. Тобто крім проблем адміністрування доступу до Інтернету користувачів-учнів, виникає також необхідність заборони доступу цієї групи користувачів до вищезгаданої інформації.

Основні фактори, що сприяють уразливості освітніх мереж є: застаріліть програмного забезпечення, а саме його недостатня оновлювальність в плані ліквідації уразливостей ОС, проблеми з оновленням антивірусних баз, недостатня обізнаність персоналу. Тому, завданням даного розділу вбачається, розглянути освітні мережі з точки зору безпеки підключення до Інтернету, та подати основні теоретичні відомості та практичні рекомендації вчителям інформатики з вищезгаданих питань.

Завдання КСІБ, при наявності підключення НКК до Інтернету - доповнити цю систему необхідними засобами захисту внутрішньої мережі від віддалених атак та шкідливих програм. Це можливо лише при вірному поєднанні антивірусного захисту комп'ютера-шлюзу при його роботі в Інтернет, а також при встановленні на ньому відповідного програмного забезпечення, наприклад, міжмережного екрану (firewall).

Питання безпеки.

Система Internet при проектуванні не планувалася як захищена мережа, тому її проблемами є*:*

- *легкість перехоплення даних* і фальсифікація адрес у мережі. Основна частина трафіку Internet - це нешифровані дані. E-mail, паролі і файли можуть бути перехоплені шляхом використання доступних програм;
- *вразливість засобів TCP/IP* - ряд засобів TCP/IP спроектовано незахищеними, і це може бути скомпрометовано кваліфікованими зловмисниками; засоби, що використовуються для тестування, особливо вразливі;
- *відсутність політики* - багато сайтів сконструйовані так, що надають широкий доступ до себе з боку Internet, не враховуючи можливості зловживання цим доступом; багато сайтів дозволяють роботу більшій кількості сервісів TCP/IP, ніж їм необхідно для роботи, і не намагаються обмежити доступ до інформації про свої комп'ютери,якою можуть скористатися зловмисники; [20, с.103]

При підключенні локальної мережі до Інтернету, безперечно, ризики зростають. Необхідно обов'язково приймати заходи для захисту локальної мережі. Основні вимоги до захисту:

- Захист локальної мережі від віддаленого НСД з боку глобальної мережі;
- Втаємничення інформації про структуру внутрішньої мережі і її компонентів від користувачів глобальної мережі;
- Розмежування доступу в захищену мережу і із захищеної мережі в глобальну.

2.3.1. Підключення локальної мережі до Інтернету.

Для підключення локальної мережі використовуються два основних методи підключення: постійне та тимчасове. Постійне вимагає швидкісного каналу зв'язку з провайдером, а також наявності маршрутизатора та спеціального модему. Тимчасове є більш дешевим та найчастіше використовується в умовах навчальних закладів: за допомогою звичайного модему та телефонного кабелю.

При підключенні локальної мережі до Інтернету один з комп'ютерів виступає в якості **шлюзу:** через модем чи іншим способом зв'язується з Internet, а інші комп'ютери з'єднуються з Інтернетом через нього. Для повноцінної роботи в Інтернеті шлюз повинен мати реальний IP-адрес, в іншому випадку він не отримає ззовні ні одного IP-пакету. Як правило, реальний IP-адрес виділяється лише комп'ютеру-шлюзу, що має безпосереднє з'єднання з Інтернетом. При підключенні через модем IP-адреса призначається йому динамічно, з пулу провайдера. При постійному з'єднані він постійний.

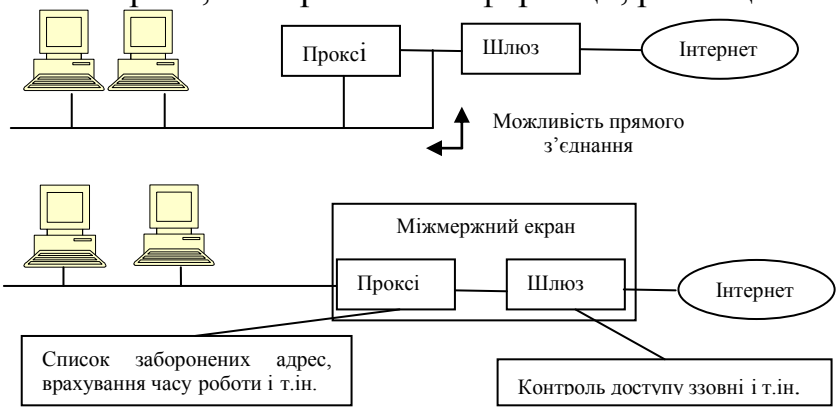
Після підключення різниця між статичними і динамічними адресами щезає. На комп'ютері-шлюзі будуть працювати як програми-клієнти, так і програми-сервери. Причому програми-сервери будуть доступними з обох мереж – як із Internet, так і із локальної мережі. (Небажані з'єднання ззовні можуть бути відключені засобами безпеки, які ми розглянемо далі). Це відбувається тому, що у комп'ютера- шлюзу принаймні два мережних інтерфейси: наприклад, модем і мережна карта. І відповідно дві IP-адреси одна «реальна», що призначається контролеру віддаленого доступу, друга внутрішня, що призначається мережній карті у локальній мережі. Така конфігурація доступу до Інтернет, вирішує відразу два завдання:

- Економляться дефіцитні IP-адреси;
- Забезпечується захист комп'ютерів локальної мережі (крім комп'ютера шлюзу)

2.3.2. Організація безпечного колективного доступу до Інтернету.

Однак така архітектура не дозволяє іншим комп'ютерам в мережі з'єднуватися з Інтернетом. Для того щоб таке з'єднання стало можливим, необхідне використання спеціальної програми-посередника, яка носить назву проксі-сервер.

Проксі-сервер (від анг. Proxy – замісник, уповноважений) – це сервер-посередник, до чиїх завдань входить обробка запитів, що приходять від комп'ютерів своєї мережі, на отримання інформації, розміщеної зовні неї.



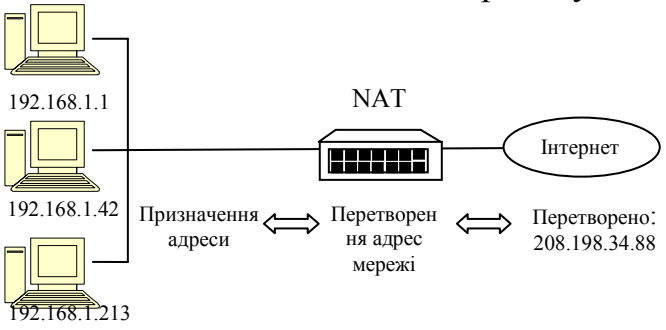
Мал.5. Проксі-сервер та міжмережний екран.

Кешування.

Якщо документ чи зображення повністю передані по мережі від www-серверу програмі-браузеру, то браузер зберігає їх в своєму кеші (кеш знаходиться в окремому підкаталозі браузера на диску). Якщо користувач в подальшому запитає той самий документ, то перед тим як заново перекачувати файл по мережі, браузер перевірить, чи є він в кеші. Якщо документ на сервері не новіший ніж документ у кеші, то користувачу буде запропоновано документ з кешу, що суттєво збільшить швидкість роботи. Розмір кешу обмежений. Він встановлюється користувачем в налаштуваннях браузера. Нові документи витісняють старі. Однією з функцій проксі-сервера є кешування web-сторінок.

Перетворення мережних адрес.

Одним з найрозповсюдженіших способів сховати конфігурацію внутрішньої мережі є використання одних адрес для внутрішніх систем і перетворення їх при зв'язку з Інтернетом. Такий механізм носить назву перетворення мережних адрес (NAT – Network Address Translation). Необхідність в NAT виникла внаслідок швидкого розвитку Інтернет і неспроможності забезпечити всі системи в Інтернеті унікальною адресою.



Мал.6.Перетворення мережних адрес.

Тому для внутрішніх мереж використовується зарезервований простір IP-адрес.

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.0.0 – 192.168.255.255

Не кожній організації є потреба застосовувати NAT. Однак якщо NAT буде використовуватися, необхідно включити відповідне формулювання в правила політики в найбільш загальному вигляді.

Адреси внутрішньої мережі мають залишатися схованими. Коли системи запитують доступ до інших мереж, сховані адреси повинні перед передачею бути перетворенні в легальні зареєстровані адреси.

2.3.3. Міжмережний екран (Firewall).

Міжмережний екран (МЕ) – це спеціалізований комплекс міжмережного захисту, який також називають брандмауером чи системою firewall. Зазвичай МЕ захищає внутрішню мережу організації від «вторгнення» із глобальної мережі. Тоді він має розміщуватися між мережею, яку захищає, та потенційно ворожою мережею. Для більшості організацій МЕ є необхідною умовою забезпечення безпеки внутрішньої мережі.

Можна класифікувати МЕ за такими ознаками.

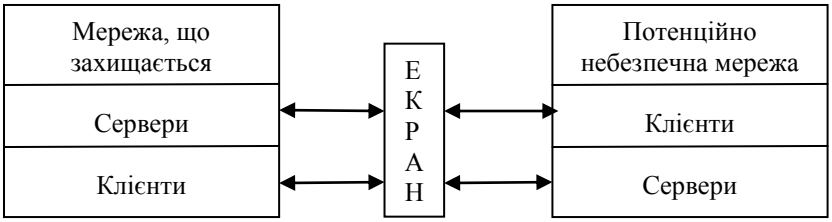
За функціонуванням на рівнях моделі OSI:

- Пакетний фільтр (екрануючий маршрутизатор – screening router);
- Шлюз сеансового рівня (екрануючий транспорт)
- Прикладний шлюз (application gateway)
- Шлюз експертного рівня (statefull inspection firewall)

За виконанням:

- Апаратно-програмний
- Програмний.
- Фільтрування трафіку.
- Фільтрування інформаційних потоків.

При розгляді будь-якого питання, що стосується мережних технологій, основою служить еталонна модель ISO/OSI. Міжмережеві екрани також доцільно класифікувати по тому, на якому рівні виробляється фільтрація - канальному, мережному, транспортному чи прикладному. Відповідно, можна говорити про концентратори, що екранують, (рівень 2), маршрутизатори (рівень 3), про транспортне екранування (рівень 4) і про прикладні екрани (рівень 7). Існують також комплексні екрани, що аналізують інформацію на декількох рівнях.



Мал.7. Екран як засіб розмежування доступу.

Міжмережевий екран - це напівпроникна мембрана, що розташовується між що захищається (внутрішньою) мережею і зовнішнім середовищем (зовнішніми мережами чи іншими сегментами корпоративної мережі) і контролює всі інформаційні потоки у внутрішню мережу і з неї (Мал. 7).

Контроль інформаційних потоків складається в їхній фільтрації, тобто, у вибірковому пропущенні через екран, можливо, з виконанням деяких перетворень і повідомленням відправника про те, що його даним у пропуску відмовлено. Фільтрація здійснюється на основі набору правил, попередньо завантажених в екран і мережні аспекти, що є вираженням політики безпеки організації.

2.3.4. Політика безпеки Інтернет.

Мета політики безпеки для Internet - прийняти рішення про те, як організація передбачає захищатися. Політика інформаційної безпеки, зазвичай, складається з двох частин - загальних принципів і конкретних правил роботи. Загальні принципи визначають підхід до безпеки в Internet. Правила ж визначають, що дозволено, а що заборонено. Правила можуть бути доповнені конкретними процедурами та різними рекомендаціями.

Політика безпеки Інтернет повинна передбачувати:

- Ліміти об’єму інформації для кожного користувача.
- Правила антивірусного захисту, які неможливо минути. Наприклад заборона завантаження активного коду.
- Ввести правила змістовного фільтрування запитів користувачів, щоб заборонити доступ неповнолітніх до деяких сайтів, що містять шкідливу інформацію.
- Ввести правила фільтрування вхідного трафіку, захисту топології внутрішньої мережі, захисту портів Інтернет-шлюзу.

Захист внутрішнього навчального веб-сервера.

Особливої уваги потребує інформація навчального призначення, що подається у вигляді внутрішнього web-серверу. Цей веб-сервер може бути розроблений для організації учбового процесу з багатьох предметів. А тому важливо, щоб був визначений працівник, який несе відповідальність за загальну політику безпеки веб-сервера, займається вставкою документів у корпоративне дерево, їхньою корекцією і видаленням. Крім того, автори окремих розділів (вчителі з конкретних предметів) не повинні мати прав на модифікацію корпоративного дерева. Важливим, з точки зору безперервності учбового процесу, є захист вихідних документів від модифікації учнями-користувачами, що не забороняє їх копіювання.

Інформація про дітей на шкільних веб-сайтах.

Кількість шкільних веб-сайтів з кожним роком зростає, та, не зважаючи на це, багато вчителів ще недостатньо розуміють, яку саме інформацію про дітей можна розміщувати на них. Реалії сьогодення показують, що особисті дані учнів (і не тільки в електронному вигляді) можуть бути використані зловмисниками, що ставить під загрозу особисту безпеку дітей. Тому краще на шкільних вебсайтах розміщати фотографії дітей тільки за згодою батьків і тільки групові. Якщо на шкільному веб-сайті розміщена інформація про учнів, то варто вказувати лише загальні факти з життя дитини (його інтереси, хобі, заслуги) не вказуючи його фізичну адресу, адресу електронної пошти (без дозволу батьків), телефон, повне ім'я й іншу особисту інформацію.

Посилання на інші ресурси на шкільному веб-сайті.

Якщо школа на своєму веб-сайті розміщає посилання на будь-який інший, нешкільний сайт, потрібно обов'язково перевірити, чи є цей сайт прийнятним для відвідування його учнями. Корисним в такому випадку є використання «спливаючих вікон», які попереджують про перехід в небезпечну зону: це убезпечить вас від ситуації, коли зміст ресурсу змінився на неприйнятний.

Навіть якщо керівництво Вашої школи вирішить, що таке спливаюче вікно з попередженням не потрібно, учителі повинні розповісти батькам, що дітям можуть бути доступні нешкільні сайти і, незважаючи на те, що керівництво школи рахувало, що сайти підходили для відвідування їхніми учнями в той час, коли в минулому були встановлені посилання, зміст сайтів може змінитися або вони можуть більше не діяти, тобто, школа не в змозі контролювати те, що відбувається на цих сайтах. Учитель повинен пояснити батькам і дітям, що вони відвідують такі сайти на свій страх і ризик. Тому, якщо школа не має наміру регулярно перевіряти посилання, імовірно, краще не розміщати посилання на нешкільні сайти на веб-сайті школи [44].

Додаток А. Глосарій основних термінів*.

Автентифікація (authentication) – процедура перевірки відповідності пред'явленого ідентифікатора об'єкта КС на предмет належності його цьому об'єкту; встановлення або підтвердження автентичності.

Авторизація (authorization) – надання повноважень; встановлення відповідності між повідомленням (пасивним об'єктом) і його джерелом (створене його користувачем або процесом).

Авторизація (authorization) – надання повноважень; встановлення відповідності між повідомленням(пасивним об'єктом) і його джерелом (створене його користувачем або процесом).

Авторизований користувач (authorized user) – користувач, що володіє певними повноваженнями.

Адміністратор (administrator, administrative user) – користувач; роль якого включає функції керування КС/або КЗЗ.

Адміністратор безпеки (security administrator) – адміністратор, відповідальний за дотримання політики безпеки.

Аналіз ризику (risk analysis) – процес визначення загроз безпеці інформації та їх характеристик, слабких сторін КСЗІ (відомих і припустимих), оцінки потенційних збитків від реалізації загроз та ступеня їх прийнятності для експлуатації АС.

Атака (attack) – спроба реалізації загрози.

Вразливість системи (system vmneraMity) – нездатність системи протистояти реалізації певної загрози або сукупності загроз.

Втрата інформації (information leakage) – неконтрольоване поширення інформації, що веде до її несанкціонованого одержання.

Доступність (availability) – властивість ресурсу системи (КС, послуги, об'єкта КС, інформації), яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не очікуючи довше заданого (малого) проміжку часу, тобто коли він знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли він йому потрібний.

Журнал реєстрації (audit trail) – упорядкована сукупність реєстраційних записів, кожен з яких заноситься КЗЗ за фактом здійснення контрольованої події.

*Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу. Навч. посібник /За ред. С.Г.Лаптева. - К.: Вид-во Європ. ун-ту, 2001. - С.155-173.

Загроза (threat) – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС.

Запит на доступ (access request) – звернення одного об'єкта КС до іншого з метою отримання певного типу доступу.

Засоби захисту (protection facility) – програмні, програмно-апаратні та апаратні засоби, що реалізують механізми захисту.

Захист від несанкціонованого доступу; захист від НСД (protection from unauthorized access) – запобігання або істотне утруднення несанкціонованого доступу до інформації.

Заходи забезпечення безпеки (safeguards) – послуги, функції, механізми, правила і процедури, призначені для забезпечення захисту інформації.

Ідентифікація (identification) – процедура присвоєння ідентифікатора об'єкту КС або встановлення відповідності між об'єктом і його ідентифікатором; упізнання.

Інцидент – будь-яке порушення правил інформацыйної безпеки, встановленої в організації.

Комплекс засобів захисту; КЗЗ (trusted computingbase; TCB) – сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації.

Захищена комп'ютерна система; захищена КС (trusted computer system, trusted computer product) – комп'ютерна система, яка здатна забезпечувати захистоброблюваної інформації від певних загроз.

Квота (quota) – обмеження можливості використання певного ресурсу КС користувачем або процесом.

Керування доступом (access control) – сукупність заходів з визначення повноважень і прав доступу, контролю за дотриманням ПРД.

Ключ (key) – конкретний стан деяких параметрів алгоритму криптографічного перетворення, що забезпечує вибір одного перетворення із сукупності можливих для даного алгоритму.

Комплексна система захисту інформації; КСЗІ – сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в АС.

Компрометація (compromise) – порушення політики безпеки; несанкціоноване ознайомлення.

Комп'ютерний вірус (computer virus) – програма, що має здатність до самовідтворення і, як правило, здатна здійснювати дії, які можуть порушити функціонування КС і/або зумовити порушення політики безпеки.

Конфіденційність інформації (information confidentiality) – властивість інформації, яка полягає в тому, що вона не може бути отримана неавторизованим користувачем і/або процесом.

Криптографічне перетворення – перетворення даних, яке полягає в їх шифруванні, вироблення імітовставки або цифрового підпису.

Люк (trap door) – залишені розробником недокументовані функції, використання яких дає можливість обминути механізми захисту.

Механізми захисту (security mechanism) – конкретні процедури і алгоритми, що використовуються для реалізації певних функцій і послуг безпеки.

Міжмережний екран (firewall) – комплекс програмно-апаратних засобів, які здійснюють весь комплекс захисту внутрішньої мережі від іншої (потенційно ворожої).

Модель порушника (user violator model) – абстрактне формалізоване або неформалізоване описання порушника.

Модифікація (modification) – зміна користувачем або процесом інформації, що міститься в об'єкті.

Несанкціонований доступ до інформації; НСД до інформації (unauthorized access to information) – доступ до інформації, здійснюваний з порушенням ПРД.

Ознайомлення (disclosure) – одержання користувачем або процесом інформації, що міститься в об'єкті.

Пароль (password) - секретна інформація автентифікації, що являє собою послідовність символів, яку користувач повинен ввести через обладнання вводу інформації, перш ніж йому буде надано доступ до КС або до інформації.

Повноваження (privilege) – права користувача або процесу на виконання певних дій, зокрема, на одержання певного типу доступу до об'єктів.

Політика безпеки інформації (information security policy) – сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації.

Порушник (user violator) – користувач, який здійснює несанкціонований доступ до інформації.

Правила розмежування доступу; ПРД (access mediation rules) – частина політики безпеки, що регламентує правила доступу користувачів і процесів до пасивних об'єктів.

Право доступу (access right) – дозвіл або заборона здійснення певного типу доступу.

Програмна закладка (program bug) – потайно впроваджена програма або недокументовані властивості програмного забезпечення, використання яких може призвести до обходу КЗЗ і/або порушення політики безпеки.

Проникнення (penetration) – успішне подолання механізмів захисту системи.

Проксі-сервер(proxy) – це сервер-посередник, до чиїх завдань входить обробка запитів, що приходять від комп’ютерів своєї мережі, на отримання інформації, розміщеної зовні неї.

Реєстрація (audit, auditing) – послуга, що забезпечує збирання й аналіз інформації щодо використання користувачами і процесами функцій і об'єктів, контрольованих КЗЗ.

Ризик (risk) – функція ймовірності реалізації певної загрози, виду і величини завданих збитків.

Розмежування доступу (access mediation) – сукупність процедур, що реалізують перевірку запитів на доступ і оцінку на підставі ПРД можливості надання доступу.

Розшифрування даних (data decryption) – процес перетворення шифртексту у відкритий текст.

Санкціонований доступ до інформації (authorized access to information) – доступ до інформації, що не порушує ПРД.

Список доступу (access control list) – перелік користувачів і/або процесів з зазначенням прав доступу їх до об'єкта КС, з яким пов'язаний цей перелік.

Список повноважень (privilege list, profile) – перелік об'єктів з зазначенням прав доступу до них з боку користувача або процесу, з яким пов'язаний цей перелік.

Стійкість до відмов (fault tolerance) – послуга, що забезпечує здатність КС продовжувати функціонування в умовах виникнення збоїв і відмов окремих компонентів.

Тип доступу (access type) – суттєвість доступу до об'єкта, що характеризує зміст здійснюваної взаємодії, а саме: проведені дії, напрям потоків інформації, зміни в стані системи (наприклад, читання, запис, запуск на виконання, видаляння, дозапис).

*Троянський кін*ь (Trojan horse) – програма, яка, і будучи авторизованим процесом, крім виконання документованих функцій, здатна здійснювати приховані дії від особи авторизованого користувача в інтересах розробника цієї програми.

Цілісність інформації (information integrity) – властивість інформації, яка полягає в тому, що вона не може бути модифікована неавторизованим користувачем і/або процесом.

Цілісність системи (system integrity) – властивість системи, яка полягає в тому, що жоден її компонент не може бути усунений, модифікований або доданий з порушенням політики безпеки.

Шифрування даних – процес зашифрування або розшифрування.

Додаток В. Схеми.

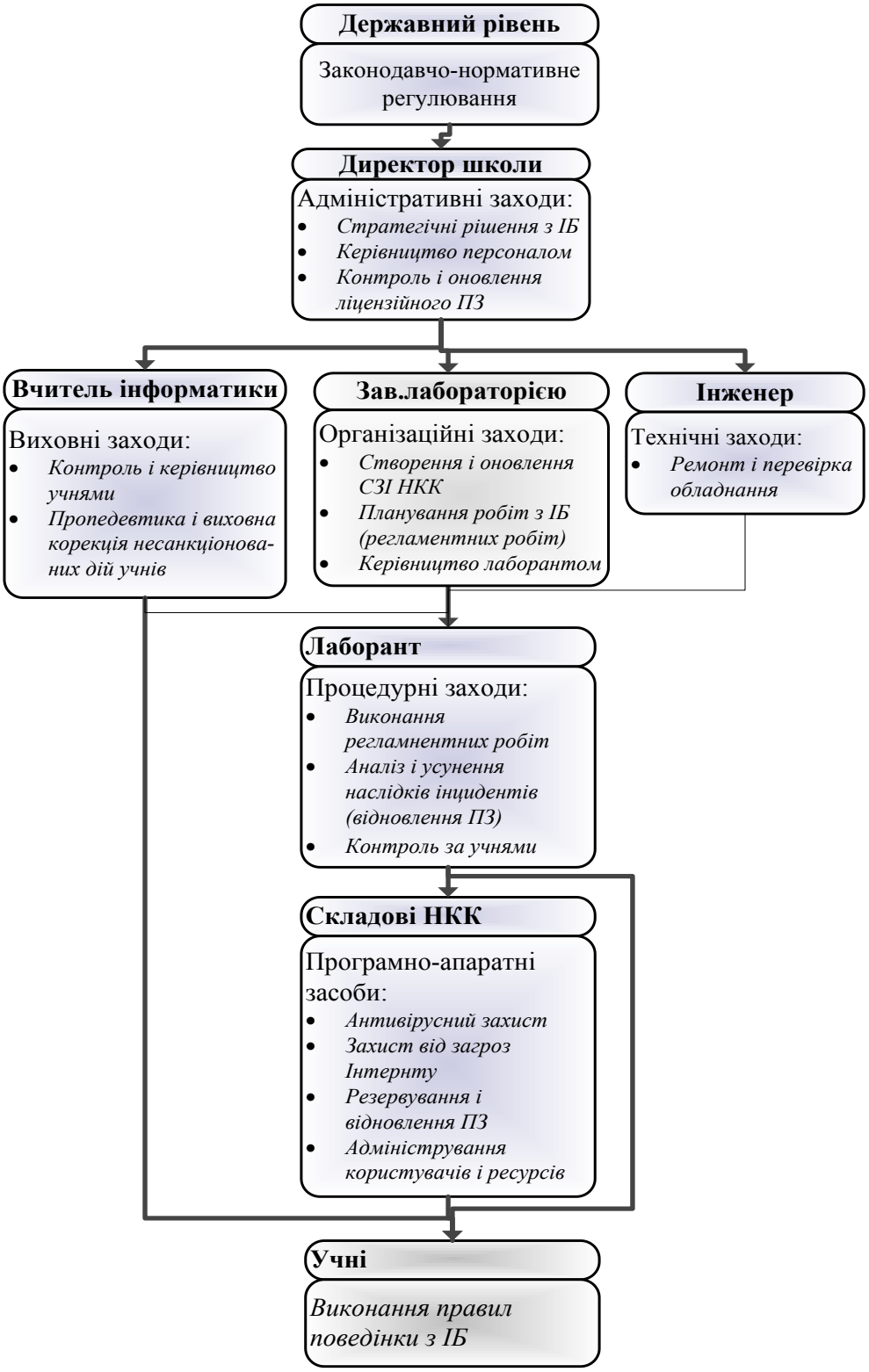


Схема 1. Розподіл заходів з інформаційної безпеки серед персоналу

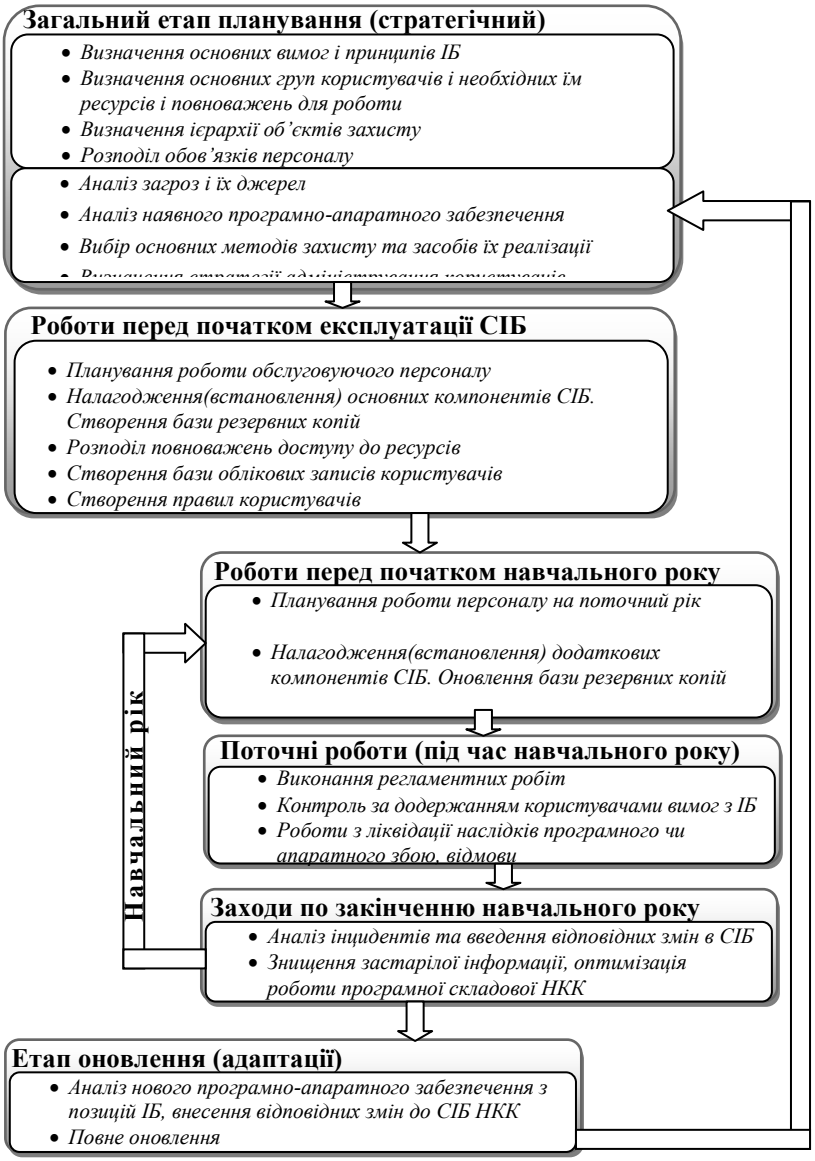


Схема 2. Планування заходів з ІБ на всіх етапах життєвого циклу СІБ НКК.

Додаток С. Приклади правил інформаційної безпеки.

Правила роботи учнів у кабінеті інформаційно-комунікаційних технологій (доповнення правилами інформаційної безпеки)

Обов'язки користувачів по реєстрації в системі:

1. Для реєстрації в системі ми повинні ввести по запиту своє користувацьке ім'я (логін) та пароль;
2. Якщо ви ввели некоректно пароль три рази, то ваш обліковий запис буде заблоковано, розблокувати її може лише лаборант (вчитель інформатики);
3. Ви ніколи не повинні записувати свій пароль;
4. Ви ніколи не повинні повідомляти будь-кому свій логін чи пароль;
5. Якщо ви забули свій пароль, необхідно особисто отримати новий у лаборанта.

Робота в комп'ютерному класі:

1. Комп'ютерне обладнання та програмне забезпечення класу призначене лише для навчальних цілей і повинно використовуватися лише для цього;
2. Не можна приносити на носіях та завантажувати на жорсткі диски комп'ютерів заборонену інформацію (порнографію, що демонструє жорстокість), стороннє програмне забезпечення.
3. У класі підтримується стандартна конфігурація всіх робочих станцій, користувачам забороняється змінювати цю конфігурацію, якщо дана зміна не передбачена навчальним завданням.

Обов'язки користувача Internet:

1. Підключення школи до Інтернету повинно використовуватися лише для навчання;
2. Забороняється використання комп'ютерів шкільного класу та підключення до Інтернету для ігор, отримання та збереження забороненої інформації (порнографії, що демонструє жорстокість), стороннього програмного забезпечення.
3. Користувачі повинні знати що комунікації Internet не є конфіденційними. Користувачі не повинні передавати по мережі інформацію, яка містить їх конфіденційну інформацію: прізвище, адреса, телефон, особисті фотографії та іншу інформацію, розголошення якої може нанести їм шкоду.
4. Користувачі не повинні завантажувати з Internet програмне забезпечення та активні компоненти web-сторінок, а всі дані що завантажуються ними з Internet повинні пройти антивірусну перевірку. Дані, що завантажуються учнями з Internet повинні бути навчального призначення і мати розмір, що не перевищує встановлений у навчальному закладі ліміт.

Контроль та дослідження мережних даних.

1. Керівництво школи попереджує, що воно має право досліджувати і знищувати будь-які дані, що зберігаються на комп'ютерах та мережних системах. Також введеться контроль за діями учнів: візуальний і електронний. Якщо зібрані факти будуть свідчити про порушення

користувачем правил інформаційної безпеки чи законів, то вони можуть бути використані як підстава для дисциплінарного покарання.

Правила антивірусного захисту:

1. На всіх комп'ютерах встановлено антивірусне програмне забезпечення. Обов'язок користувачів полягає у сприянні заходам антивірусного захисту.
2. Користувачі повинні перевіряти всі дані при кожному їх завантажені з будь-якого джерела. Також необхідно перевіряти будь-який переносний носій перед його відкриттям на наявність вірусів.
3. Користувачі повинні сприяти оновленню антивірусних баз, а також ніколи не перешкоджати та не вивантажувати з оперативної пам'яті антивірусні програми.
4. Користувачі не повинні створювати, запускати, передавати чи демонструвати ніяких комп'ютерних кодів, які можуть нанести шкоду системам обробки даних чи інформації, що в них зберігається.

Кодекс моральної поведінки у віртуальному середовищі:

1. Не можна поширювати інформацію, що може містити наклеп, образу будь-якої людини за національними, расовими, статевими, фізичними та іншими прикметами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

Нормативні документи та закони.

1. Положення про кабінет інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів // Інформатика. - 2005. - №2-3. - С. 3-8.
2. Методичні рекомендації щодо облаштування і використання кабінету інформатики та інформаційно-комунікаційних технологій навчання загальноосвітніх навчальних закладів // Інформатика. - 2005. - №2-3. - С. 9-32.
3. Правила безпеки під час навчання в кабінетах інформатики навчальних закладів системи загальної середньої освіти // Інформатика. - 2005. - №2-3. - С. 33-37.
4. Вимоги до специфікації навчальних комп'ютерних комплексів // Комп'ютер у школі та сім'ї. - 2007. - №4. - С. 50-51.
5. Правила використання комп'ютерних програм у навчальних закладах. Затверджено наказом Міністерства освіти і науки України від 2 грудня 2004 року N 903.
6. Державна програма “ Інформаційні та комунікаційні технології в освіті і науці ” на 2006–2010 роки. Затверджено постановою кабінету міністрів від 7 грудня 2005 р. № 1153.
7. Закон України "Про інформацію" від 02.10.1992р. - №2657-XII.
8. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 31.05.2005 № 2594-IV
9. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки» від 9.01.2007 № 537-V.

Навчальні посібники з інформаційної безпеки.

10. Анин Б. Защита компьютерной информации СПБ: БХВ – СПб.; 2000. – 368с.
11. Бармен С. Разработка правил информационной безопасности: Пер. с анг. – М.: «Вильямс», 2002. – 208 с.: ил. – ISBN 5-8459-0323-8
12. 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.
13. Галатенко В.А. Основы информационной безопасности // Интернет-университет информационных технологий [Електронный ресурс]. – Режим доступа: – http://www.intuit.ru
14. Глосарій з курсу «Захист інформації в інформаційних системах» для студентів спеціальності 7.080401 усіх форм навчання. – Харьків: ХДЕУ, 2004. – 16 с.
15. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. – Киев: “Корнійчук”, 2000 – 152 с.
16. Домарев В.В. Защита информации и безопасность компьютерных систем. – К.; Издательство “Диа-Софт”, 1999. – 480 с.

17. Корченко О.Г., Морозов А.С. Захист та зламування програм.: Навчальний посібник. К.: НАУ, 2001. – 84 с. Библ.81.

18. Косарев В.М., Петренко А.Н. Информационная безопасность: организация защиты програм и даннях. Учебное пособие. – Днепропетровск: Изд. ДУЭП, 2003. –152 с.

19. Крысин А. В. Информационная безопасность. Практическое руководство.: - М.: СПАРРК, К.: ВЕК+, 2003. – 320 с.

20. Лужецький В.А., Северин Л.І., Гульчак П.Ю., Кожухівський А.Д. Основи організаційного захисту інформації. Навчальний посібник. – Вінниця: ВНТУ, 2005. – 148 с.

21. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учебное пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 280 с.: ил.

22. Мамаев М., Петренко С. Технологии защиты информации в интернете. Специальный справочник. – СПб.: Питер, 2002. – 848 с.

23. Медведев Н.Г., Москалюк Д.В. Аспекти информационной безопасноети виртуальних частных сетей. Учебное пособие. - К.: Изд-во Европ.ун-та, 2002. - 95 с

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

25. Михаэль А. Бэнкс. Информационная защита ПК: Пер. с анг.. – К.: ВЕК+, М.: Энтроп, Спб.: Корона-Принт 2001. –272 с.

26. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. – М.: Горячая линия - Телеком, 2006. – 544 с.: ил.

27. Партыка Т.Л., Попов И.И. Информационная безопасность. Учебное пособие для студентов среднего професионального образования. – М.; Форум-Инфра-М, 2002. –368 с.

28. Петраков А.В. Основы практической защиты информации. 3-е изд. Учебн. Пособие. М.: Радио и связь, 2001. – 368 с.;ил.

29. Пономаренко В.С., Журавльова І.В., Туманов В.В. Основи захисту інформації. Навчальний посібник. – Харьків: Вид.ХДЕУ, 2003. – 176 с.

30. Устенко І.В. Системи захисту інформації: Навч.посібник. Миколаїв: НУК, 2006. – 68 с.

31. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: издатель Молгачева С.В., 2001, 352 с., ил.

32. Великий тлумачний словник сучасної української мови / Укладач і головний редактор В.Т.Бусел. – К.; Ірпінь: ВТФ «Перун», 2004. – 1440 с.

Програмне забезпечення.

33. Андреев А.В. и др. Microsoft Windows Server. Русская версия / Под общ. ред. А.Н. Чекмарева и Д.Б. Вишнякова. – Спб.: БХВ – Санкт-Петербург, 2000. – 960 с.: ил.

34. Виллеттт Эдвард, Каммингс Стив. Office XP. Библия пользователя. «Вильямс», 2002. – 848 с.: ил.

35. Мінухін С В. Лабораторний практикум з навчальної дисципліни "Комп'ютерні мережі". Навчально-практичний посібник для студентів напряму підготовки 0804 "Комп'ютерні науки" всіх форм навчання / С. В. Мінухін, В. Ю. Жукарєв; [Заг. редакція докт екон. наук, професора. С. Пономаренка. – Харків: Вид. ХНЕУ, 2007. – 212 с (Укр. мов.)

36. Пєтух А.М., Войтко В.В., Бевз С.В., Яремко С.А. Мережі ЕОМ. Лабораторний практикум. -Вінниця: ВНТУ, 2003 - 125 с.

37. Сетевые операционные системы/ В.Г. Олифер, Н.А. Олифер. – Спб.: Питер, 2002. – 544 с.: ил.

38. Симпсон Алан, Андердал Брайан Windows XP. Библия пользователя. Пер. с англ.: – М.: Издательский дом «Вильямс», 2004. – 704 с.: ил.

39. Уильям Р. Станек Microsoft Windows XP Professional. Справочник системного администратора. Пер. с англ.: М.: Издательский дом «Русская редакция», 2002. –448 с.: ил.

40. Эффективная работа: Windows XP / Э. Ботт, К. Зихерт. – СПб.: Питер, 2003. – 1069 с: ил.

Проблеми інформаційної безпеки в школі.

41. Інформаційна безпека України: сутність та проблеми. [Електронный ресурс]. – Режим доступа: http://bezpeka.com/ru/lib/spec/art12.html

42. Безопасность детей в Интернете. Microsoft, 2006. – [Електронный ресурс]. – Режим доступа: http://www.microsoft.com/rus/athome/security/children/default.mspx

43. Серебреникова М. Компьютерная этика. – [Електронный ресурс]. – Режим доступа: http://www.ourtx.com/?a=289

44. Личный интернет. Учителям о проблемах информационной безопасности в образовании. [Електронный ресурс]. – Режим доступа: http://www.content-filtering.ru

45. Прохоров А. «Приличный» Интернет в школе и дома // КомпьютерПресс. – №2. – 2007. [Електронный ресурс].– Режим доступа: http://www.compress.ru/article.aspx?id=17262&iid=799

46. Полат Е.С. Проблема информационной безопасности в образовательных сетях рунет. [Електронный ресурс].– Режим доступа: http://www.ioso.ru/distant/library/publication/infobez.htm

47. Поляков В.П. Аспекты информационной безопасности в курсе информатики и информационных технологий // Школьные технологии. – 2006. – №6 – С.177-179.

48. Мошкин В.Н., Чередниченко А.И. Проблема информационной безопасности в содержании школьного образования [Електонный ресурс]. – Режим доступа: http://www.uni-altai.ru/engine/download.php?id=502

49. Ершов Д.А.Информационная безопасность личности как цель социально-педагогической деятельности // Учитель Российской школы – ключевая фигура модернизации образования, интернет конференция 1 марта – 1 июня 2008 г. [Електонный ресурс]. – Режим доступа: http://modern-obraz08.livejournal.com/2634.html

50. Давлетханов М. Статья про Интернет в школе. [Електонный ресурс]. – Режим доступа: http://www.guru-soft.ru/entensysarticles

51. Онландия. [Електонный ресурс]. – Режим доступа: http://www.onlandia.org.ua

52. Журин А.А. Информационная безопасность как педагогическая проблема // Педагогика. – 2001.– №4. – С.49-54.

53. Чусавитина Н.Г. Элективный курс «Основы информационной безопасности» // Информатика и образование. - 2007. - N 4. - С. 41-56.