DOI: https://doi.org/10.36910/6775-2524-0560-2022-47-12
УДК 622 004.056.
Каганюк Олексій Казимирович. к.т.н., доцент
https://orcid.org/0000-0003-4616-8768
Чернящук Наталія Леонідівна, д.пед.н., професор
https://orcid.org/0000-0002-3178-8377
Бурчак Ігор Несторович, к.т.н., доцент
https://orcid.org/0000-0003-2662-6442

АНАЛІЗ АПАРАТНИХ ТА ПРОГРАМНИХ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ ДО ІНФОРМАЦІЙНОГО КАНАЛУ ПЕРЕДАЧІ ДАНИХ

Каганюк О.К., Чернящук Н.Л., Бурчак І.Н. Аналіз апаратних та програмних методів захисту інформації від несанкційного доступу до інформаційного каналу передачі даних. В даній статті проводиться аналіз та обгрунтуванню щодо захисту інформаційного каналу по використання як технічних засобів та і програмного забеспечення захисту від несанкційного доступу.

Ключові слова: захисті інформації**,** несанкціонований .доступ, паралельні атаки, мережева розвідка, ехо-тестування, передача даних

Kaganyuk O.K., Chernyashchuk N.L, Burchak I. N. Analysis of hardware and software methods for protecting information from unauthorized access to the information channel of data transmission. This article analyzes and justifies the main provisions for the protection of the information channel on the use of both technical, means and software protection against unauthorized access.

Keywords: information security, unauthorized access, parallel attacks, network intelligence, echo-testing, data transmission

Вступ

З середини 20-го століття інформація є загальнонауковим поняттям, яке включає наступні основні положення:

Інформація, за допомогою якої здійснюється обмін між людьми, між оператором та складним апаратним пристроєм, а також між об'єктами, що працюють в автоматичному режимі.

Передача інформації у тваринному та рослинному світі. Біологічний процес передачі інформації та у багатьох інших аспектах нашого неосяжного всесвіту.

Ґрунтуючись на філософському трактуванні, можна впевнено сказати, що інформація існує незалежно від людини і є матерією. У даному конкретному випадку, ми будемо розглядати наявність інформації, яку застосовуватимемо для управління різних технологічних процесів з використанням останньої в апаратних блоках та пристроях [1].

Постановка задачі

Проблема полягає в тому, що цю інформацію слід доставити на об'єкт у заданій формі без спотворення та втрат, для афективного управління різноманітними об'єктами і не тільки.

Ґрунтуючись на фундаментальних трактуваннях, виділимо із загального поняття інформації, таке поняття як безпеку зберігання даної інформації, так і безпеку формування безпечного каналу передачі цієї інформації.

У доктрині інформаційної безпеки України розглядається безпека захищеності національних інтересів в інформаційному просторі у сфері, що визначається сукупністю збалансованих всебічних інтересів суспільства та держави. У більшості випадків, трактування інформаційної безпеки ми розумітимемо як стан захищеності інформації, що підтримує інфраструктуру від випадкових обурю вальних впливів різного характеру, що впливають на життєдіяльність соціуму.

Нам необхідно визначитися, а в чому полягає захист інформації та інформаційного каналу передачі даних. Це, як правило, комплекс правових, організаційних та технічних способів та дій, які перешкоджають поширенню загроз та забезпечують передумови зменшення наслідків у процесі передачі інформації в інформаційних системах. Необхідно відзначити, що інформаційна безпека, це одна із складових інформаційних підсистем загальної інформаційної системи, що бере участь у життєвому циклі [2].

Огляд та аналіз існуючих методів захисту інформації

Для аналізу інформаційної безпеки передачі даних по інформаційному каналу сформулювати основні положення визначають положення безпеки. Нас будуть цікавити такі параметри:

• швидкість переходу від традиційних носіїв (паперових) зберігання інформації до електронних технологій;

• використання локальних обчислювальних мереж;

• створення глобальних мереж із розширеним доступом до інформаційного ресурсу;

• необхідно враховувати зростання складності програмного забезпечення у системах управління та передачі даних.

На даний момент важко оцінити збитки компанії або держави у разі витоку або втрати інформації в нормальних режимах експлуатації або форс-мажорних обставинах. Необхідно враховувати некомпетентність технічного персоналу, крадіжку даних, промисловий шпигунство, технічні неполадки роботи апаратури та інше. Забезпечення безпеки інформаційних технологій є комплексною проблемою, яка охоплює як правове регулювання, так і технологічні процеси як якісну експлуатацію апаратного обладнання, сертифікацію, сучасну технологію розвитку та інше.Класифікація атак

Розглянемо, які існують методи несанкціонованого доступу захисту інформації. Для цього нам необхідно з визначенням, а що таке несанкціонований доступ до інформації – це сукупність прийомів та порядок проведення дій з метою передачі (прийому) достовірної інформації, що охороняється і не підлягає знищенню під час передачі інформації каналом зв'язку.

Нам необхідно з'ясувати і визначитися на основних моментах, на яких може спертися зловмисник для викрадення інформації при несанкціонованому доступі.

Сюди ми включимо такі основні положення на наш погляд:

• це насамперед отримати секретну інформацію про свого конкурента.

• вносити зміни до інформаційного потоку передачі даних з використанням своїх корисливих інтересів;

• вплинути створення втрат шляхом знищення цінної інформації.

Для детального розгляду цього питання нам необхідно провести класифікацію. Від яких атак потрібно проводити захист інформаційного каналу. Провівши детальний аналіз, ми виділимо найхарактерніші типи мережевих атак. Почнемо з найпростішої атаки. Це так звані сніфер пакети це прикладна програма, в якій використовується мережна карта, що працює у випадковому режимі. Такий режим роботи дозволяє проводити перехоплення IP-пакетів, які беруть участь у заданому сегменті. Ця ситуація можлива тоді, коли замовник (хакер) виконує функції справжнього користувача. Таку ситуацію можна створити двома способами.

По-перше, хакер має можливість скористатися IP-адресою, що знаходиться в заданому функціональному діапазоні IP-адреси.

По-друге, хакер має можливість скористатися уповноваженою зовнішньою адресою, яка має доступ до явних мережевих ресурсів.

Наступний вид атаки це парольні атаки. При проведенні хакером паралельних атак доводиться застосовувати ряд різних методів, наприклад, простий перебір (brute force attack), «троянський кінь», IP – спуфінг та сніффер пакети.

Атаки на рівні програм можуть здійснюватися декількома засобами.

Так, наприклад, найпоширеніший приклад атак полягає у використанні добре відомих нестійкосте серверного програмного забезпечення (sendmail, HTTP, FTP). На жаль, більшість хакерів мають доступ, що дає змогу вдосконалювати свої професійні можливості.

Мережева розвідка. Це збір інформації про інформаційний канал передачі даних через конкретну мережу за допомогою загальнодоступних програм. Виконуючи цю атаку, хакер прагне якнайбільше дізнатися інформації про користувача, який йому цікавий. Такого типу атаки проводяться, як правило, на рівні приватних підприємців. , оскільки інформаційний захист знаходиться на низькому рівні. Такі атаки здійснюються у вигляді запиту DNS. За допомогою запитів DNS вдається зрозуміти, хто є власником того чи іншого домену, які адреси відносяться до конкретного домену.

Відлуння – тестування (ping sweep) адрес. Відлуння – тестування проводиться після того, коли визначено DNS, це дозволяє визначити реально працюючі хости в даному середовищі. Отримавши список хостів, що працюють, стає можливим провести сканування портів. Після цього складається повний список послуг, що надаються цим хостам. За підсумками отриманої інформації зловмисник здійснює аналіз показників додатків що працюють на даних хостах. Отримана інформація дозволяэ здійснити злом інформаційного каналу.

Dos-напад. Цей напад характеризується тим, що може вплинути на недоступність комп'ютерних ресурсів користувачеві.

Для того, щоб завадити каналу передачі інформації, можна використовувати насичений метод атак комп'ютерного або мережевого обладнання великою кількістю зовнішніх запитів. Внаслідок такої атаки обладнання не в змозі відповісти користувачеві. Цей процес протікає дуже повільно і не цікавить.

Якщо атака була проведена з одночасно працюючих великої кількості IP-адрес то таку атаку називаю розподіленою DDOS атакою.

Метою дослідження є визначення основних методів та систем захисту інформації від несанкціонованого доступу інформації і не тільки в такому напрямку, а й інших модифікаціях захисту інформації.

Функції та завдання захисту інформації повинні визначати не лише склад, а й структуру захисту, модифікацію системи та інше. Наведемо основні компоненти, які мають увійти до нашого розгляду. На малюнку 1 представлений зразок основних видів загроз, які можуть впливати на цілісність інформації, її конфіденційність, надійність передачі даної інформації та працездатності каналу зв'язку і комп'ютерної системи в цілому. Ця таблиця має право на озвучку після детального аналізу та вивчення технічного матеріалу у цьому напрямку. Це може бути і суб'єктивна думка, але вона має право бути, це наше розуміння та обґрунтування такого аналізу, який буде розкритий у наступному.

Реалізацію зі створення методів та систем захисту інформації можна розділити на наступні складові:

• загрози, реалізація яких здійснюється за постійної участі людини (зловмисника); яка перешкоджає чи бажає отримати доступ до інформації;

• загрози, реалізація яких здійснюється за допомогою технічних засобів, які можуть бути встановлені зловмисником передачі інформації;

• загрози, що здійснюються за допомогою шкідливого програмного забезпечення відповідними комп'ютерними програмами без участі людини.

Ці завдання щодо забезпечення захисту від загроз, можна вважати, що вони однотипні, у зв'язку з тим, для спрощення аналізу їх можна об'єднати і виразити в наступному форматі:

• розробити засоби для неможливого несанкціонованого доступу до ресурсів комп'ютерних систем та мереж;

• розробити технічні та програмні засоби, які не дозволили б використовувати комп'ютерні ресурси, якщо доступ до них все ж таки здійснився;

• своєчасно виявляти факт здійснення несанкціонованого доступу з усуненням причин, а також наслідків їх реалізації.

• загрози, що здійснюються за допомогою шкідливого програмного забезпечення відповідними комп'ютерними програмами без участі людини.

Ці завдання щодо забезпечення захисту від загроз, можна вважати, що вони однотипні, у зв'язку з тим, для спрощення аналізу їх можна об'єднати і виразити в наступному форматі:

• розробити засоби для неможливого несанкціонованого доступу до ресурсів комп'ютерних систем та мереж;

• розробити технічні та програмні засоби, які не дозволили б використовувати комп'ютерні ресурси, якщо доступ до них все ж таки здійснився;

• своєчасно виявляти факт здійснення несанкціонованого доступу з усуненням причин, а також наслідків їх реалізації.

Реалізацію зі створення методів та систем захисту інформації можна розділити на наступні складові:

• загрози, реалізація яких здійснюється за постійної участі людини (зловмисника); яка перешкоджає чи бажає отримати доступ до інформації.

Класифікація та обґрунтування методів захисту інформації

Проведемо аналіз можливих порушень у роботі комп'ютерних систем, які б створити загрозу таємної інформації. Такі загрози можна розбити на такі компоненти. Це морально, правові, адміністративні, технічні та програмні [1,5]. Для кращого розуміння та аналізу ми зробили маленьке припущення, яке дозволить виявити основний напрямок вирішення цієї проблеми. Покладаючись на сучасні розробки технічного та програмного забезпечення, можна обґрунтовано сказати, що нам слід рухатись з удосконалення сучасних систем саме у цьому напрямі.

Морально – етичні засоби.

До цієї групи відносяться норми поведінки, які традиційно склалися або складаються з поширення ЕОМ, мереж тощо. Ці норми здебільшого є обов'язковими і затверджені у законодавчому порядку, та їх невиконання часто призводить до падіння авторитету і престижу людини, групи осіб, організації чи країни. Морально-моральні норми бувають як неписаними, і оформленими у певний статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів

ЕОМ США. Необхідно визначитись на які норми нам необхідно спиратися та взяти за базові для умов роботи у сфері ІТ – технологій.

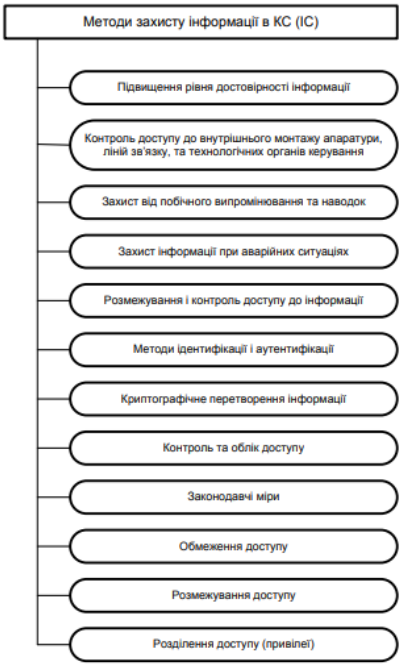

Рисунок 1 – Методи захисту інформації у комп'ютерній системі

Правові засоби захисту — чинні закони, ДСТУ, укази та інші нормативно – технічні акти та документи, що регламентують правила використання інформації та відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання ІТ.

Перехід до інформаційного суспільства вимагає вдосконалення кримінального та цивільного законодавства, а також судочинства, що діє в Україні. Сьогодні спеціальні закони прийняті у всіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються та вдосконалюються. Порівняти їх між собою практично неможливо, оскільки кожен закон слід розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження та інше. У проекті міжнародної угоди, боротьби з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи (див. матеріали сайту http://www.coe.int), було внесено зміни [1].

Загальною тенденцією, яку можна простежити, є посилення кримінальних законів щодо комп'ютерних злочинців. Так, вже сьогодні в Гонконгу максимальним покаранням за такий злочин, якщо він призвів до виведення з ладу 1С або Web-сайту, є 10 років ув'язнення. Для порівняння, в Кримінальному кодексі України незаконне втручання у роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти тисяч гривень або виправними роботами терміном до двох років, або обмеженням волі на той самий термін.

Адміністративні (організаційні)

Дані засоби захисту інформації регламентують процеси функціонування 1С, можливість використання даного ресурсу, практичну діяльність технічного та допоміжного персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою виключити або не допустити порушень безпеки. Вони охоплюють:

• заходи, що передбачаються під час проектування, будівництва та облаштування об'єктів охорони (з огляду на вплив стихії, протипожежну безпеку, охорону приміщень, пропускний режим, прихований контроль за роботою працівників тощо);

• заходи, що здійснюються при проектуванні, розробці, ремонті та модифікації обладнання та програмного забезпечення (сертифікація всіх використовуваних технічних та програмних засобів; суворе санкціонування, розгляд та затвердження всіх змін тощо);

• заходи, що здійснюються під час підбору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх з порядком роботи з конфіденційною інформацією та ступенем

відповідальності за його недотримання; створення умов, за яких персоналу було б невигідно або неможливо допускати зловживання тощо);

• розробку правил обробки та зберігання інформації, а також стратегії її захисту (організація обліку, зберігання, використання та знищення документа та носіїв з конфіденційною інформацією; розмежування доступу до інформації за допомогою паролів, профілів повноважень тощо; розробка адміністративних норм та системи)) покарань за їх порушення тощо) [3].

Адміністративні засоби

Адміністративні засоби захисту є неодмінною частиною захисту, їх значення обумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації. Особливістю адміністративних засобів є те, що в основному вони припускають застосування інших видів захисту, таких як (технічний або програмний захист) і тільки в такому дуалізмі здатні забезпечити досить високий і надійний захист. У той самий час велика кількість адміністративних правил тяжить працівників і зменшує надійність захисту, оскільки написані інструкції із захисту просто виконуються технічним персоналом[3, 5]..

Засоби фізичного (технічного) захисту інформації

Даний метод передбачає електронно-механічні пристрої, механічні, або електронні, а також споруди та матеріали, призначені для захисту від несанкціонованого доступу та завантаження інформації, що передається по каналу зв'язку та попередження її втрати внаслідок порушення працездатності всіх компонентів інформаційної системи (ІС), стихійних лих, саботаж, диверсій тощо. [3,5]: До цієї групи належать:

Засоби захисту кабельних мереж.

За даними різних досліджень, саме збої кабельної мережі викликають більше половини відмов поточного інформаційного зв'язку. Найкращим засобом запобігти подібним збоям є побудова структурованої кабельної системи (СКС), в якій використовуються кабелі з однаковими технічними параметрами для передачі даних в ІС, сигналів від датчиків пожежної безпеки, відеоінформаційних датчиків, датчиків охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» передбачає, що кабельну систему об'єкта можна розділити на кілька рівнів. Що дозволить більш обґрунтовано підійти до захисту окремих компонентів, що виконуються у блоковому виконанні, з контрольною світлодіодною індикацією для визначення безпечного проходження інформації на окремій ділянці залежно від її призначення та розміщення. Для ефективної організації надійної роботи СКС слід дотримуватись вимог міжнародних стандартів;

Засоби захисту електроживлення.

Американські дослідники з компанії Best Power після п'яти років досліджень проблем безпеки електроживлення дійшли висновку [1,2] що на кожному комп'ютері в середньому 289 разів на рік виникають порушення харчування, тобто майже один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації, у разі тимчасових відключень електроенергії, або стрибків напруги в мережі є необхідність використовувати установку джерел безперебійного живлення. Різноманітність технічних та споживчих характеристик технічних засобів дозволяє вибрати пристрій, який відповідатиме адекватним конкретним вимогам даного об'єкта. В умовах підвищених вимог до працездатності ІС є необхідність використання аварійного електрогенератора або резервних ліній електропередач, які рознесені для підключення до різних осередків підстанції.

Засоби архівації та дублювання інформації.

При великих обсягах інформації, доцільно організовувати окремий спеціалізований сервер для зберігання архівованих даних. Якщо архівна інформація має велику цінність, її слід зберігати в спеціальному приміщенні, що охороняється, або в секретній кімнаті з обмеженим доступом технічного персоналу. На випадок пожежі або стихійного лиха слід зберігати дублікати найцінніших архівів в іншому приміщенні (будівлі) можливо, в іншому районі або іншому місті, тобто, зберігати інформацію в різних географічних місцях. Тим самим підвищується надійність оберігання секретної інформації і не тільки.

Засоби захисту від різних природних явищ, що виникають при роботі технічних засобів, засоби виявлення апаратури, що прослуховує, у вигляді «жучків», електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів і т.д. [5]. До цієї ж групи можна віднести матеріали, що забезпечують безпеку зберігання та транспортування носіїв інформації, а також захист від копіювання. Переважно це спеціальні тонко плівкові матеріали, що мають змінну колірну гаму або голографічні мітки, що

наносяться на документи та предмети (у тому числі і на елементи комп'ютерної техніки), що дозволяють ідентифікувати достовірність об'єкта та проконтролювати доступ до нього[5].

Як було зазначено, найчастіше технічні засоби захисту реалізуються разом із програмним забезпеченням.

Програмні засоби захисту інформаційних каналів

Програмні засоби захисту забезпечують ідентифікацію та аутентифікацію користувачів відповідно до розмежування доступу до ресурсів. Відповідно до повноважень користувачів здійснюється реєстрація подій в ІС, криптографічний захист інформації, захист від комп'ютерних вірусів тощо.

Розглядаючи програмні засоби захисту інформації, доцільно зупинитись на стеганографічних методах. Слово «стеганографія» означає прихований лист, що не дозволяє сторонній особі дізнатися про його існування. Одна з перших згадок про застосування таємнопису, який датується V століттям до н. е. Сучасним прийомом є випадок роздруківки на ЕОМ договорів з малопомітними спотвореннями обрисів окремих знаків тексту – так вносилася шифрована інформація про умови складання договора.[4].

Розглянемо, за якими принципами необхідно визначити базування стенографії.

По-перше, аудіо та відео файли, а також файли з цифровими зображеннями, які можна певною мірою змінити в цифровому форматі без втрати функціональності, використовуючи теорему Шеннона [3]. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних методів, їх можна нанести на цифрові носії знайшовши лише за допомогою спеціального програмного забезпечення – цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, що генеруються на основі секретних ключів. Такі знаки можуть забезпечити справжність чи недоторканність документа, ідентифікувати автора чи власника, перевірити права дистриб'ютора чи користувача, навіть якщо файл було оброблено чи спотворено.[4] .

Щодо впровадження засобів програмно-технічного захисту в 1С, розрізняють два основні способи:

- додатковий захист – засоби захисту є доповненням до основних програмних та апаратних засобів комп'ютерної системи;
- вбудований захист – механізми захисту реалізуються у вигляді окремих компонентів 1С або розподілені за іншими компонентами системи. [1, 5].

Перший спосіб є більш гнучким, його механізми можна додавати та вилучати за потребою, але за його реалізації можуть виникнути проблеми забезпечення сумісності. засобів захисту між собою та з програмно-технічним комплексом 1С. Вбудований захист вважається більш надійним і раціональним, але жорстким, оскільки виникають труднощі при внесенні змін. Таке доповнення характеристик дозволяє комбінувати з іншими компонентами захисту.

Аналіз та обґрунтування програмних методів захисту інформації.

Найкращий захист інформації програмними засобами – це використання антивірусних програм, спеціальних програм, які призначені для виявлення та знищення комп'ютерних вірусів.

Антивірусні програми діляться кілька видів.

Програми-детектори проводять пошук сигнатур вірусів. Недоліком програм-детекторів є те, що вони можуть знаходити ті віруси, які відомі розробникам, отже, вони швидко застарівають. І знову доводиться робити дослідження з розробки нових програм захисту інформації. Цей процес триває постійно та залежить від високої кваліфікації обслуговуючого технічного персоналу цього підрозділу. Деякі програми-детектори можна настроювати на нові типи вірусів, проте неможливо екстраполювати нову розробку програми, яка могла б виявити будь-який заздалегідь невідомий вірус. Відтак негативний результат перевірки програмою-детектором не гарантує відсутність вірусів. Багато детекторів мають режими лікування чи знищення заражених файлів, вони виконують функції лікарів.

Більш розширеними можливостями наділені програми-лікарі (фаги) Вони не тільки знаходять заражені вірусами файли, але й лікують їх (тобто видаляють з файлу тіло програми-вірусу), повертаючи їх у початковий стан. Перед лікуванням файлів програма очищує оперативну пам'ять. Серед фагів відокремлюють поліфаги – програми-лікарі, які призначені для пошуку та знищення великої кількості вірусів. Як і детектори, програми-лікарі потребують постійного оновлення.

Програми-ревізори дозволяють запам'ятовувати початковий стан програм, каталогів та системних областей, коли комп'ютер не заражений вірусом, а згодом, періодично або за бажанням користувача, звіряється поточний стан системи з вихідним. Як правило, перевірка здійснюється одразу після завантаження операційної системи. Одночасно контролюється довжина файлу, його контрольна сума, дата, час модифікації та інші параметри. Деякі програми-ревізори можуть при цьому виявляти стелю вірусів. Гібриди програм-ревізорів та лікарів можуть не тільки виявляти зміни, але й повертати

файли та системні області у вихідний стан. Вони більш універсальні, оскільки можуть захистити від вірусу, невідомого на час їх створення, якщо він використовує стандартний механізм зараження.

Наступним цікавим об'єктом є ***програми-фільтри*** («сторожа», «монітори» — резиденти), призначені виявлення підозрілих дій під час роботи комп'ютера. Після отримання відповідного повідомлення, користувач може дозволити або скасувати виконання операції. Деякі програми-фільтри перевіряють програми, що викликаються до виконання, та копіювання файлів. Недоліком подібних програм є їхня «набридливість», можливі конфлікти з іншим програмним забезпеченням, а переваги — виявлення вірусів на ранній стадії, що дозволяє мінімізувати втрати.

Програми-вакцини («імунізатори») модифікують програми та диски таким чином, що ця операція не відбивається на роботі різних програм. Але вірус, від якого виробляється вакцинація, вважає їх зараженими. Це дуже неефективний спосіб захисту. Вакцини мають обмежене використання. Їх можна застосувати лише проти відомих вірусів. Жоден з типів антивірусних програм не надає стовідсоткового захисту, тому слід дотримуватися загальних вимог та прав щодо використання останніх розробок антивірусних лабораторій.

Правильний антивірус повинен поєднувати багатосторонні властивості, і згодом його використання призведе до достатньої безпеки комп'ютера та його даних і мережі в цілому.

Результати досліджень

На базі проведеного аналізу захисту несанкційного доступу до інформації, експерименти проводилися в КП «Водоканал», у процесі проведення переддипломної практики, вибірково були проведені дослідження захисту інформації. У результаті аналізу різних методів захисту інформації, були визначені основні методи підвищення інформації по каналу зв'язку. Передумови гібридного застосування методів захисту, виявилися більш ефективними, на відміну від одиночного обраного методу.

У разі використання гібридного методу, необхідно враховувати конкретну специфіку роботи підприємства. Диференційовано підходити до вибору систем захисту, звертаючи увагу на пріоритети та зіставляючи гасло «ціна – якість». Це дозволить як афективно використовувати системи захисту, а й підвищити надійність експлуатації комп'ютерної системи загалом.

Висновки. У своєму становленні сучасні інформаційні технології пройшли кілька етапів розвитку, у кожному з яких спостерігалося переважання окремих видів та способів обробки інформації. На даний момент найбільше доцільно для захисту інформації необхідно використовувати гнучкі технології, що передбачають різні методи захисту, де будуть використані не тільки технічні методи захисту, а й програмне забезпечення, операційна система та інше. Оскільки загрози мають не статичний, а динамічний характер, слід зазначити, що основні методи захисту інформації від загроз – це забезпечення структурної, тимчасової інформаційної та функціональної надмірності комп'ютерних ресурсів та використання спеціальних програмних та апаратних засобів захисту – це антивірусні програмні пакети, або програми – антивіруси.

Список бібліографічного опису

1. Петров В.А. Інформаційна безпека. Захист інформації від несанкціонованого доступу в автоматизованих системах / Петров В.А., Піскарьов С.А., Шеїн А.В. – М. : Изд-во Ореан, 1998. – 534 с

2. Антонюк А.О. Основи захисту інформації в автоматизованих системах/ А. О. Антонюк. – К.: КМ Академія, 2006. – 244 с

3. Виявлення та розслідування злочинів, що вичиняються у сфері інформаційних технологій: Наук.-практ.посіб./ За заг.ред.проф. Я.Ю.Кондратьєва. – К., 2004.

4. Каганюк О.К. Технічні та програмні засоби шифрування, дешифрування. Конспект рекцій для здобувачів першого (бакалаврського) рівня вищої освіти освітньо-професійної програми «Кібербезпека» галузь знань 12 Інформаційні технології спеціальності 125 Кібербезпека денної та заочної форм навчання / уклад. О.К.Каганюк – Луцьк : Луцький НТУ, 2021. – 84 с..

5 ДСТУ 3396.0-96 Захист інформації. Технічний захист інформації .Основні положення .

Reference

1. Petrov V.A. Information security. Information about unauthorized access in automated systems / Petrov V.A., Piskarov S.A., Shein A.V. - M.: Publishing house Orean, 1998 .-- 534 s

2. Antonyuk A.O. Basics of obtaining information in automated systems / A.O. Antonyuk. - K .: KM Academy, 2006 .-- 244 p.

3. Investigation and analysis of maladies, as well as in the sphere of information technologies: Science and practice, / For the editorial board of prof. Ya.Yu. Kondrat'va. - K., 2004.

4. Kaganyuk O.K. Technical and software for encryption, decryption. Synopsis of recitals for the education of the first (bachelor's) level of education in the educational and professional programs of «Cybersecurity». O.K. Kaganyuk - Lutsk: Lutsk NTU, 2021 .-- 84 p ..

5. DSTU 3396.0-96 Information protection. Technical information manager.