Комунальний заклад освіти   
«Дніпровський ліцей інформаційних технологій при Дніпровському національному університеті імені Олеся Гончара»

**ВИПУСКНА РОБОТА**

**Тема: «**Комп'ютерні засоби захисту інформації»

**Виконав:**

Ліцеїст 11-В класу

Мордак Антон Олександрович

**Керівник:**

Ентін Йосиф Абрамович, \_\_\_\_\_\_\_\_

Дніпро

2021

**Актуальність:** У сучасному світі інформація  – головний ресурс, який відіграє незмінно важливу роль у будь якій сфері людської діяльності і від степені її конфеденційності залежить її цінність, тому захист першочерговою задачею. В роботі розглянуті комп’ютерні засоби безпеки інформації на прикладі електронного довідника та перевірочні тести до нього для закріплення знань з теми.

**Мета роботи**: Було розробити електронний довідник з теми: «Комп’ютерні засоби безпеки інформації», та тести до нього, де буде наочно та доступно пояснено, яким чином ви можете захистити свою інформацію.

# ЗМІСТ

# ВСТУП

Проблема забезпечення [інформаційної](https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) безпеки є актуальною з тих пір, як [люди](https://ua-referat.com/%D0%9B%D1%8E%D0%B4%D0%B8) почали обмінюватися [інформацією](https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F), накопичувати її і зберігати. У всі часи виникала необхідність надійного збереження найбільш важливих досягнень людства з метою передачі їх нащадкам. [Аналогічно](https://ua-referat.com/%D0%90%D0%BD%D0%B0%D0%BB%D0%BE%D0%B3%D1%96%D1%8F_2) виникала необхідність обміну конфіденційною інформацією і надійної її захисту.  
 У сучасному суспільстві проблема інформаційної безпеки особливо актуальна, оскільки [інформація](https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) стала частиною [життя](https://ua-referat.com/%D0%96%D0%B8%D1%82%D1%82%D1%8F) сучасного суспільства. [Розвиток](https://ua-referat.com/%D0%A0%D0%BE%D0%B7%D0%B2%D0%B8%D1%82%D0%BE%D0%BA) сучасного суспільства багато в чому визначається тими інформаційними процесами, які в ньому протікають.  
 Швидко розвиваються [інформаційні технології](https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97) вносять помітні зміни в життя суспільства. [Інформація](https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) стала товаром, який можна придбати, продати, обміняти. При цьому вартість інформації часто у багато разів перевершує вартість апаратних засобів, в яких вона зберігається. Від ступеня безпеки [інформаційних](https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%8F) технологій залежить благополуччя, а часом і життя багатьох людей.  
 З початком масового застосування комп'ютерів проблема інформаційної безпеки набула особливої ​​гостроти. З одного боку, комп'ютери стали носіями інформації і, як наслідок, одним із каналів її отримання як санкціонованого, так і несанкціонованого. З іншого боку, комп'ютери як будь-технічний пристрій схильні збоїв і помилок, які можуть призвести до втрати інформації. Під інформаційною безпекою розуміється захищеність інформації від випадкового або навмисного втручання, що завдає шкоди її власникам або користувачам.

# Причини комп’ютерних злочинів

Захист інформації є однією з вічних проблем. Протягом історії людства способи розв'язання цієї проблеми визначались рівнем розвитку технологій. У сучасному інформаційному суспільстві технологія відіграє роль активатора цієї проблеми — комп'ютерні злочини стали характерною ознакою сьогодення. Комп'ютерними називають злочини, пов'язані з втручанням у роботу комп'ютера, і злочини, в яких комп'ютери використовуються як необхідні технічні засоби. Серед причин комп'ютерних злочинів і пов'язаних з ними викрадень інформації головними є такі:

• швидкий перехід від традиційної паперової технології зберігання та передавання інформації до електронної за одночасного відставання технологій захисту інформації, зафіксованої на машинних носіях;

• широке використання локальних обчислювальних мереж, створення глобальних мереж і розширення доступу до інформаційних ресурсів;

• постійне ускладнення програмних засобів, що викликає зменшення їх надійності та збільшення кількості уразливих місць.

Сьогодні ніхто не може назвати точну цифру загальних збитків від комп’ютерних злочинів, але експерти погоджуються, що відповідні суми вимірюються мільярдами доларів. Серед основних статей варто виокремити такі:

• збитки, до яких призводить ситуація, коли співробітники організації не можуть виконувати свої обов'язки через непрацездатність системи (мережі);

• вартість викрадених і скомпрометованих даних;

• витрати на відновлення роботи системи, на перевірку її цілісності, на доробку уразливих місць тощо.

Варто також враховувати й морально-психологічні наслідки для користувачів, персоналу і власників інформації. Що ж до порушення безпеки так званих «критичних» додатків у державному і військовому управлінні, атомній енергетиці, медицині, ракетно-космічній галузі та у фінансовій сфері, то воно може призвести до тяжких наслідків для навколишнього середовища, економіки і безпеки держави, здоров'я і навіть для життя людей.

# Види порушення безпеки

Економічні та юридичні питання, приватна та комерційна таємниця, національна безпека — усе це зумовлює необхідність захисту інформації.

Згідно із Законом України «Про захист інформації в автоматизованих системах» захист інформації — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. У літературі вживаються також споріднені терміни «безпека інформації» та «безпека інформаційних технологій». Забезпечення безпеки інформаційних технологій являє собою комплексну проблему, яка охоплює правове регулювання використання IT, удосконалення технологій їх розробки, розвиток системи сертифікації, забезпечення відповідних організаційнотехнічних умов експлуатації.

Розв'язання цієї проблеми потребує значних витрат, тому першочерговим завданням є співвіднесення рівня необхідної безпеки і витрат на її підтримку. Для цього необхідно визначити потенційні загрози, імовірність їх настання та можливі наслідки, вибрати адекватні засоби і побудувати надійну систему захисту. Базовими принципами інформаційної безпеки є забезпечення цілісності інформації, її конфіденційності і водночас доступності для всіх авторизованих користувачів. Із цього погляду основними випадками порушення безпеки інформації можна назвати такі:

• несанкціонований доступ — доступ до інформації, що здійснюється з порушенням установлених в 1C правил розмежування доступу;

• витік інформації — результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

• втрата інформації — дія, внаслідок якої інформація в 1C перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;

• підробка інформації — навмисні дії, що призводять до перекручення інформації, яка має оброблятися або зберігатися в 1C;

• блокування інформації — дії, наслідком яких є припинення доступу до інформації;

• порушення роботи ІC — дії або обставини, які призводять до спотворення процесу обробки інформації. Причини настання зазначених випадків такі:

• збої обладнання (збої кабельної системи, перебої в електроживленні, збої серверів, робочих станцій, мережних карт, дискових систем тощо);

• некоректна робота програмного забезпечення (втрата або змінювання даних у разі помилок у ПЗ, втрати даних унаслідок зараження системи комп'ютерними вірусами тощо);

• навмисні дії сторонніх осіб (несанкціоноване копіювання, знищення, підробка або блокування інформації, порушення роботи 1C, спричинення витоку інформації);

• помилки обслуговуючого персоналу та користувачів (випадкове знищення або змінювання даних; некоректне використання програмного та апаратного забезпечення, яке призводить до порушення нормальної роботи системи, виникнення вразливих місць, знищення або змінювання даних, порушення інтересів інших законних користувачів тощо; неефективно організована система захисту; втрата інформації через неправильне зберігання архівних даних тощо);

• навмисні дії обслуговуючого персоналу та користувачів (усе сказане у попередніх двох пунктах, а також ознайомлення сторонніх осіб із конфіденційною інформацією).

# Основні особливості комп’ютерних злочинів

Основні особливості комп’ютерних злочинів:

• встановлення факту вчинення злочину. На відміну від традиційних, правоохоронець не може виявити труп, відсутність матеріальних цінностей на складі, пошкоджений автомобіль. Всі сліди злочину знаходяться на матеріальних носіях комп’ютера, який може знаходиться на значній відстані від потерпілої особи;

• відсутність міждержавних кордонів для злочинців (якщо злочин вчиняється з використанням глобальної комп’ютерної мережі) та існування декількох місць вчинення злочину (при несанкціонованому доступі до банківських комп’ютерних систем місцем вчинення злочину слід вважати саму банківську систему, що була атакована, так і місце знаходження комп’ютера, з якого здійснювали доступ, а також місце надходження коштів для отримання готівки).

Загалом найбільшу загрозу безпеці інформації становлять люди, тому саме їхні навмисні чи випадкові дії потрібно передбачати, організовуючи систему захисту. Співробітники служб комп'ютерної безпеки поділяють усіх порушників на чотири групи стосовно жертви:

* сторонні, які не знають фірму;
* сторонні, які знають фірму, та колишні співробітники;
* співробітники-непрограмісти;
* співробітники-програмісти.

Межа між програмістами та простими користувачами з погляду небезпечності останнім часом стирається. Останні становлять більшість співробітників, звичайно мають базову комп'ютерну підготовку і можуть скористатися спеціальним програмним забезпеченням, яке має дружній інтерфейс і доступне на піратських CD-ROM, у спеціальних розділах BBS і на сайтах Інтернет та FidoNet. За твердженнями експертів, тільки чверть співробітників цілком лояльна, чверть настроєна до фірми вороже і не має моральних обмежень, лояльність решти залежить від обставин. Тому нелояльні співробітники, які мають доступ до комп'ютерів і знайомі з системою, становлять серйозну загрозу ІС.

Передусім це організаційна проблема, технологія тут може відігравати тільки допоміжну роль. Для позначення різних категорій комп'ютерних злочинців використовуються різноманітні терміни: «хакери», «кракери», «пірати», «шкідники».

**Хакери (хекери)** — це узагальнююча назва людей, які зламують комп'ютерні системи. Часто цей термін застосовується і до «програмістів-маніяків» — за однією з легенд, слово «hack» уперше стало застосовуватись у Массачусетському технологічному інституті для позначення проекту, який не має видимого практичного значення і виконується виключно заради задоволення від самого процесу роботи. У більш вузькому розумінні слово «хакер» позначає тих, хто одержує неправомочний доступ до ресурсів тільки для самоствердження.

Останнє відрізняє хакерів від професійних зламувачів — **кракерів (або «крекерів»),** які є серйозними порушниками безпеки, оскільки не мають жодних моральних обмежень.

Найбільш криміногенною групою є **пірати** — професіонали найвищого ґатунку, які спеціалізуються на крадіжках текстів нових комерційних програмних продуктів, технологічних ноу-хау тощо. Така робота, природно, виконується на замовлення або передбачає реального покупця. За відсутності замовлень пірат може зосередитися на кредитних картках, банківських рахунках, телефонному зв’язку.

В усіх випадках мотивація – матеріальні інтереси, а не цікавість чи пустощі. За даними дослідження корпорації IDG у 88 % випадків розкрадання інформації відбувається через працівників фірм і тільки 12 % — через зовнішні проникнення із застосуванням спеціальних засобів. У січні 2001 року на сайт! Xakep.ru з'явилось повідомлення про злом сайта ФБР (www.fbi.gov). За неперевіреними зі зрозумілих причин даними, хакери змінили структуру сайту і стерли директорію «wanted» (список найбільш небезпечних злочинців, яких розшукує ФБР), зробивши дублювальні копії файлів, про що й повідомили адміністратора сайту. Один з авторів зламу, московський програміст galblch, прокоментував свої дії так: «У принципі, злам був дрібницею — там була дірка. Першою ідеєю було просто написати адміну (адміністратору) про дірку без зламу як такого, але у зв'язку з іменитістю відомства, якому належить сайт, вирішили все ж таки розважитись». При цьому galblch вважає, що «писати програми більш цікаво, ніж шукати в них дірки, але й дірки цікаві...»

**Шкідники (вандали)** намагаються реалізувати у кіберпросторі свої патологічні схильності — вони заражають його вірусами, частково або повністю руйнують комп'ютерні системи. Найчастіше вони завдають шкоди без якої-небудь вигоди для себе (крім морального задоволення). Часто спонукальним мотивом є помста. Іноді шкідника надихає масштаб руйнівних наслідків, значно більший за можливі позитивні успіхи від аналогічних зусиль. Слід також зупинитись ще на одній групі, яка посідає проміжне місце між хакерами і недосвідченими користувачами (до речі, ненавмисні дії останніх можуть призвести до не менш тяжких наслідків, ніж сплановані атаки професіоналів). Ідеться про експериментаторів («піонерів»). Найчастіше це молоді люди, які під час освоєння інструментальних та інформаційних ресурсів Мережі і власного комп'ютера бажають вчитися тільки на власних помилках, відштовхуючись від того, «як не можна». Основну частину цієї групи становлять діти та підлітки. Головною мотивацією у цій групі є гра. З експериментаторів виходять професіонали високого класу, зокрема й законослухняні. Отже, одними з основних причин порушення безпеки інформації є незапитаність творчого потенціалу в поєднанні з неусвідомленням усіх наслідків протиправних дій. Цей фактор існує незалежно від національності або сфери професійної діяльності.

Звичайно, жодна з особистих проблем не може стати приводом для протиправної діяльності, але сьогодні суспільство тільки починає виробляти належне ставлення до комп'ютерних злочинців. Стають відомими колосальні збитки від їхньої діяльності. Розвінчується міф про хакера як про комбінацію Гудіні і Фантомаса, адже часто своїми успіхами вони завдячують не своїм навичкам, а банальним пропускам у захисті систем (звідси і нове прізвисько— «ламери»). Поширюється думка про те, що комп'ютерний злочин легше попередити, ніж потім розслідувати. Однак це не вирішує проблему повністю, адже, крім бажання розважитись і самоствердитись існує ще 5 недбалість, холодний комерційний розрахунок, прояви садизму та хворобливої уяви. Тому комп'ютерні злочини залишаються об'єктом уваги фахівців.

# Найбільш поширені види комп'ютерних злочинів

Несанкціонований доступ до інформації, що зберігається у комп'ютері, та її розкрадання. Розрізнити ці дві категорії дуже важко. Найчастіше присвоєння машинної інформації та програмного забезпечення відбувається копіюванням, що зменшує ймовірність виявлення факту крадіжки. Можливі шляхи здійснення злочину:

* використання чужого імені або пароля («маскарад»). Одержати коди та паролі законних користувачів можна придбанням (звичайно з підкупом персоналу) списку користувачів з необхідними відомостями, знаходженням подібного документа в організаціях, де контроль за їх збереженням недостатній; підслуховуванням через телефонні лінії. Відомі випадки, коли секретна інформація, і не тільки приватного характеру, відпливала через дітей
* незаконне використання привілейованого доступу
* «зламування» системи
* знаходження слабких місць у захисті системи чи недоробок у програмному забезпеченні
* використання збоїв системи
* крадіжка носіїв інформації
* читання інформації з екрана монітора
* збирання «сміття»
* встановлення апаратури підслуховування та запису, підімкненої до каналів передавання даних
* віддалене підімкнення
* модифікація програмного забезпечення

Підробка комп'ютерної інформації. Цей злочин можна вважати різновидом несанкціонованого доступу з тією різницею, що скоїти його може і стороння особа, і законний користувач, і розробник 1C. В останньому випадку може підроблятись вихідна інформація з метою імітування роботоздатності 1C і здачі замовнику свідомо несправної продукції. До цього самого виду злочинів можна віднести підтасування результатів виборів, голосувань і т. ін.

Уведення у програмне забезпечення «логічних бомб» — невеликих програм, які спрацьовують з настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Різновидом логічної бомби є «часова бомба», яка спрацьовує в певний момент часу.

Ще одним способом модифікації програмного забезпечення є таємне введення у програму (чужу або свою) «троянського коня» — команд, які дають можливість зі збереженням працездатності програми виконати додаткові, не задокументовані функції, наприклад переслати інформацію (зокрема паролі), що зберігається на комп'ютері. В останньому випадку «троянській кінь» є засобом реалізації «прихованого каналу». Виявити «троянського коня» дуже важко, оскільки сучасні програми складаються з тисяч і навіть мільйонів команд і мають складну структуру. Завдання ускладнюється, коли у програму вставляється не власне «троянській кінь» (див. вище визначення), а команди, які його формують і після досягнення поставленої мети — знищують. Також можна зазначити, що «троянські коні» можуть перебувати не тільки у програмах, айв інших файлах, наприклад в електронних листах. Один із перших завантажувальних вірусів для IBM-PC (заражав дискети 360 Kb), який стрімко розповсюдився на Заході, був написаний у Пакистані власниками компанії з продажу програмних продуктів, які хотіли з 'ясувати рівень піратського копіювання у своїй країні. Автори залишили у тілі вірусу текстове повідомлення зі своїми іменами, адресами і навіть номерами телефонів. Незважаючи на появу інших різноманітних методів захисту авторських прав, за минулий час цей приклад неодноразово наслідувався.

Розробка і поширення комп'ютерних вірусів. Напевне, сьогодні не має жодного користувача 1C, який у своїй роботі не стикався б із комп'ютерними вірусами. Прояви вірусів можуть бути різноманітними — від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів з жорсткого диска. У будьякому разі це означає порушення цілісності 1C. Сьогодні фахівці очікують появи вірусів для програмованих мікросхем і мобільних телефонів.

Злочинна недбалість у розробці, виготовленні й експлуатації комп'ютерної техніки та програмного забезпечення. Необережне використання комп'ютерної техніки аналогічне недбалому поводженню з будь-яким іншим видом техніки, транспорту і т. Його особливістю є те, що безпомилкових програм не буває в принципі. Якщо помилка призвела до наслідків, які вимагають покарання винуватців, про винність розробників свідчать:

• наявність у технічному завданні вказівок на те, що в системі може виникнути ситуація, яка призводить до збою (аварії);

• можливість створення контрольного прикладу з даними, які імітують ситуацію, що призвела до збою (аварії). Окремим випадком недбалості програмістів є створення і залишення без контролю «люків» («чорних ходів») — прихованих, не задокументованих точок входу у програмний модуль, які часто використовуються для відлагодження програми та її підтримання у процесі використання. Але «люк» може бути використаний і для зламування системи сторонньою особою, і для таємного доступу до програми самим розробником. Для виявлення «люків» слід проводити ретельний аналіз початкових текстів програм. До тяжких непередбачуваних наслідків можуть призвести й дії користувачів.

Визначити їх як халатні можна за таких ознак:

• користувач мав у своєму розпорядженні інформацію про можливі наслідки порушення інструкцій;

• виконати вимоги інструкції було можливо фізично і психологічно.

Комп'ютерні злочини в мережі Інтернет. Виокремлення цієї категорії диктується реаліями використання глобальної мережі. По-перше, Інтернет стає інструментом здійснення «звичайних» злочинів. Це промисловий шпіонаж, саботаж, поширення дитячої порнографії і т. ін. Понад третина користувачів Мережі страждає від шахрайств. Продавці еквадорської нерухомості, нафтових свердловин в Антарктиді і кокосових плантацій в Коста-Ріці, будівельники фінансово-інвестиційних пірамід і брокери, які просувають акції певних фірм і наживають на продажу цих акцій у період ажіотажу, — їхні сайти та розсилки наздоганяють сотні тисяч людей, серед яких не так вже й мало легковірних. Одним із ключових аспектів багатьох «схем» подібного роду є доступ до персональних даних користувача (див. приклад). Заповнивши анкету, людина стає потенційним об'єктом шахрайства в майбутньому, а найбільш довірливі, зокрема ті, хто надає інформацію про свою кредитну картку, страждають відразу. Відомо, що більшість шахрайств пов'язана з використанням пластикових кредитних карток і здійснюється на сайтах, що спеціалізуються на купівлі-продажу товарів. По-друге, стає все більше злочинів, пов'язаних із самим існуванням Інтернет. Крім розповсюдження вірусів та зламування сайтів можна назвати такі:

* «**нюкання**» (від англійського «nuke», ядерна зброя) -— програмна атака на іншого користувача Інтернет, у результаті якої його комп'ютер втрачає зв'язок з мережею або «зависає»;
* «**спам**» (від англійського «spam»1) або «junk mail» (пошта з мотлохом, непотрібна кореспонденція) — варіант багаторівневого маркетингу в мережі. Спаммерів можна поділити на дві групи. Першу становлять новачки, які тільки-но одержали доступ до Мережі та усвідомили, що можуть розсилати повідомлення куди завгодно і кому завгодно.
* «**винюхування**» («sniffing») — сканування пакетів, які передаються в мережі для одержання інформації про користувача (-ів);
* «**серверний трикутник**» (Web-spoofing, Web-мистифікація) — зловмисник, який проникає на сайт, змінює механізм пошуку так, що вся інформація, що її запитують користувачі, передається через якийсь інший сайт, де її, до того ж, можуть певним чином «обробити»;
* **мережні атаки**, спрямовані на «зависання» серверів («Denial of service attack», DOS-attack, атака, що спричинює відмову від обслуговування) або уповільнення їхньої роботи різними способами («повені»). Найчастіше для реалізації таких атак використо- 8 вуються пакети технологічної інформації та самі правила взаємодії серверів за мережними протоколами. Фактично єдиний спосіб створити систему, абсолютно стійку до зовнішніх впливів, — припинити будь-які її зв'язки із зовнішнім світом. А мінімальним із погляду заходом є заборона доступу до Інтернет не для службових цілей.

# Класифікація засобів захисту інформації

Залежно від можливих порушень у роботі системи та загроз несанкціонованого доступу до інформації численні види захисту можна об'єднати у такі групи: моральноетичні, правові, адміністративні (організаційні), технічні (фізичні), програмні. Зазначимо, що такий поділ є досить умовним. Зокрема, сучасні технології розвиваються в напрямку сполучення програмних та апаратних засобів захисту.

**Морально-етичні засоби.**

До цієї групи належать норми поведінки, які традиційно склались або складаються з поширенням ЕОМ, мереж і т. ін. Ці норми здебільшого не є обов'язковими і не затверджені в законодавчому порядку, але їх невиконання часто призводить до падіння авторитету та престижу людини, групи осіб, організації або країни. Морально-етичні норми бувають як неписаними, так і оформленими в деякий статут. Найбільш характерним прикладом є Кодекс професійної поведінки членів Асоціації користувачів ЕОМ США.

**Правові засоби захисту** — чинні закони, укази та інші нормативні акти, які регламентують правила користування інформацією і відповідальність за їх порушення, захищають авторські права програмістів та регулюють інші питання використання IT. Перехід до інформаційного суспільства вимагає удосконалення карного і цивільного законодавства, а також судочинства. Сьогодні спеціальні закони ухвалено в усіх розвинених країнах світу та багатьох міжнародних об'єднаннях, і вони постійно доповнюються. Порівняти їх між собою практично неможливо, оскільки кожний закон потрібно розглядати у контексті всього законодавства. Наприклад, на положення про забезпечення секретності впливають закони про інформацію, процесуальне законодавство, кримінальні кодекси та адміністративні розпорядження. До проекту міжнародної угоди про боротьбу з кіберзлочинністю, розробленого комітетом з економічних злочинів Ради Європи, було внесено зміни, оскільки його 11 розцінили як такий, що суперечить положенням про права людини і надає урядам і поліцейським органам зайві повноваження. Загальною тенденцією, що її можна простежити, є підвищення жорсткості кримінальних законів щодо комп'ютерних злочинців. Так, уже сьогодні у Гонконгу максимальним покаранням за такий злочин, якщо він призвів до виведення з ладу 1C або Web-сайту, є 10 років позбавлення волі. Для порівняння, у Кримінальному кодексі України незаконне втручання в роботу комп'ютерів та комп'ютерних мереж карається штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

**Адміністративні (організаційні)**

засоби захисту інформації регламентують процеси функціонування 1C, використання її ресурсів, діяльність персоналу, а також порядок взаємодії користувачів із системою таким чином, щоб найбільшою мірою ускладнити або не допустити порушень безпеки. Вони охоплюють:

• заходи, які передбачаються під час проектування, будівництва та облаштування об'єктів охорони (врахування впливу стихії, протипожежна безпека, охорона приміщень, пропускний режим, прихований контроль за роботою працівників і т. ін.);

• заходи, що здійснюються під час проектування, розробки, ремонту й модифікації обладнання та програмного забезпечення (сертифікація всіх технічних і програмних засобів, які використовуються; суворе санкціонування, розгляд і затвердження всіх змін тощо);

\* заходи, які здійснюються під час добору та підготовки персоналу (перевірка нових співробітників, ознайомлення їх із порядком роботи з конфіденційною інформацією і ступенем відповідальності за його недодержання; створення умов, за яких персоналу було б невигідно або неможливо припускатися зловживань і т. ін.);

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

Адміністративні засоби є неодмінною частиною захисту інформації, їх значення зумовлюється тим, що вони доступні і здатні доповнити законодавчі норми там, де це потрібно організації (див. приклад), а особливістю є те, що здебільшого вони передбачають застосування інших видів захисту (технічного, програмного) і тільки в такому разі забезпечують достатньо надійний захист. Водночас велика кількість адміністративних правил обтяжує працівників і насправді зменшує надійність захисту (інструкції просто не виконуються).

**Засоби фізичного (технічного) захисту інформації**

Це різного роду механічні, електро- або електронно-механічні пристрої, а також спорудження і матеріали, призначені для захисту від несанкціонованого доступу і викрадень інформації та попередження її втрат у результаті порушення роботоздатності компонентів 1C, стихійних лих, саботажу, диверсій і т. ін. До цієї групи відносять:

\* засоби захисту кабельної системи. За даними різних досліджень саме збої кабельної системи спричиняють більш як половину відказів ЛОМ. Найкращим способом попередити подібні збої є побудова структурованої кабельної системи (СКС), в якій використовуються однакові кабелі для організації передавання даних в 1C, сигналів від датчиків пожежної безпеки, відео-інформації від охоронної системи, а також локальної телефонної мережі. Поняття «структурованість» означає, що кабельну систему будинку можна поділити на кілька рівнів залежно від її призначення і розміщення. Для ефективної організації надійної СКС слід додержувати вимог міжнародних стандартів;

\* засоби захисту системи електроживлення. Американські дослідники з компанії Best Power1 після п'яти років досліджень проблем електроживлення зробили висновок: на 12 кожному комп'ютері в середньому 289 раз на рік виникають порушення живлення, тобто частіш ніж один раз протягом кожного робочого дня. Найбільш надійним засобом попередження втрат інформації в разі тимчасових відімкнень електроенергії або стрибків напруги в електромережі є установка джерел безперебійного живлення. Різноманітність технічних і споживацьких характеристик дає можливість вибрати засіб, адекватний вимогам. За умов підвищених вимог до роботоздатності 1C можливе використання аварійного електрогенератора або резервних ліній електроживлення, підімкнених до різних підстанцій;

\* засоби архівації та дублювання інформації. За значних обсягів інформації доцільно організовувати виділений спеціалізований сервер для архівації даних. Якщо архівна інформація має велику цінність, її варто зберігати у спеціальному приміщенні, що охороняється. На випадок пожежі або стихійного лиха варто зберігати дублікати найбільш цінних архівів в іншому будинку (можливо, в іншому районі або в іншому місті);

\* засоби захисту від відпливу інформації по різних фізичних полях, що виникають під час роботи технічних засобів, — засоби виявлення прослуховувальної апаратури, електромагнітне екранування пристроїв або приміщень, активне радіотехнічне маскування з використанням широкосмугових генераторів шумів тощо. До цієї самої групи можна віднести матеріали, які забезпечують безпеку зберігання і транспортування носіїв інформації та їх захист від копіювання. Переважно це спеціальні тонкоплівкові матеріали, які мають змінну кольорову гамму або голографічні мітки, що наносяться на документи і предмети (зокрема й на елементи комп'ютерної техніки) і дають змогу ідентифікувати дійсність об'єкта та проконтролювати доступ до нього. Як було вже сказано, найчастіше технічні засоби захисту реалізуються в поєднанні з програмними.

**Програмні засоби захисту**

забезпечують ідентифікацію та аутентифікацію користувачів (див. підрозд. 3.4.4), розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в 1C, криптографічний захист інформації, захист від комп'ютерних вірусів тощо (див. докладніше далі). Розглядаючи програмні засоби захисту, доцільно спинитись на стеганографічних методах. Слово «стеганографія» означає приховане письмо, яке не дає можливості сторонній особі взнати про його існування. Одна з перших згадок про застосування тайнопису датується V століттям до н. е. Сучасним прикладом є випадок роздрукування на ЕОМ контрактів з малопомітними викривленнями обрисів окремих символів тексту — так вносилась шифрована інформація про умови складання контракту.

**Комп'ютерна стеганографія**

базується на двох принципах. По-перше, аудіо- і відеофайли, а також файли з оцифрованими зображеннями можна деякою мірою змінити без втрати функціональності. По-друге, можливості людини розрізняти дрібні зміни кольору або звуку обмежені. Найчастіше стеганографія використовується для створення цифрових водяних знаків. На відміну від звичайних їх можна нанести і відшукати тільки за допомогою спеціального програмного забезпечення — цифрові водяні знаки записуються як псевдовипадкові послідовності шумових сигналів, згенерованих на основі секретних ключів. Такі знаки можуть забезпечити автентичність або недоторканість документа, ідентифікувати автора або власника, перевірити права дистриб'ютора або користувача, навіть якщо файл був оброблений або спотворений. Щодо впровадження засобів програмно-технічного захисту в 1C, розрізняють два основні його способи:

• додатковий захист — засоби захисту є доповненням до основних програмних і апаратні засобів комп'ютерної системи;

• вбудований захист — механізми захисту реалізуються у вигляді окремих компонентів 1C або розподілені за іншими компонентами системи.

Перший спосіб є більш гнучким, його механізми можна додавати і вилучати за потребою, але під час його реалізації можуть постати проблеми забезпечення сумісності 13 засобів захисту між собою та з програмно-технічним комплексом 1C. Вмонтований захист вважається більш надійним і оптимальним, але є жорстким, оскільки в нього важко внести зміни. Таким доповненням характеристик способів захисту зумовлюється те, що в реальній системі їх комбінують.

# Захист від комп'ютерних вірусів

Для виявлення, знищення та попередження «електронних інфекцій» можна використовувати загальні засоби захисту інформації (копіювання інформації, розмежовування доступу до неї) та профілактичні заходи, які зменшують імовірність зараження. Останніми роками з'являються апаратні пристрої антивірусного захисту, наприклад спеціальні антивіруси! плати, які вставляються у стандартні слоти розширення комп'ютера. Але найбільш поширеним методом залишається використання антивірусних програм — спеціальних програм, призначених для виявлення і знищення комп'ютерних вірусів. Антивірусні програми поділяють на кілька видів.

**Програми-детектори** здійснюють пошук сигнатур вірусів. Недоліком детекторів є те, що вони можуть знаходити тільки ті віруси, які відомі їхнім розробникам, а отже, вони швидко застарівають. Деякі програми-детектори можна настроювати на нові типи вірусів, проте неможливо розробити програму, яка могла б виявити будь-який заздалегідь невідомий вірус. Отже, негативний результат перевірки програмою-детектором не гарантує відсутності вірусів. Багато детекторів мають режими лікування або знищення заражених файлів — функції докторів.

**Програми-доктори («фаги»)** не тільки знаходять заражені вірусами файли, а й «лікують» їх (видаляють з файла тіло програ-ми-вірусу), повертаючи їх у початковий стан. Перед лікуванням файлів програма очищує оперативну пам'ять. Серед фагів виокремлюють поліфаги — програми-доктори, призначені для пошуку і знищення великої кількості вірусів. Як і детектори, програми-доктори потребують постійного оновлення.

**Програми-ревізори** запам'ятовують початковий стан програм, каталогів і системних областей, коли комп'ютер не заражений вірусом, а згодом, періодично або за бажанням користувача, порівнюють поточний стан системи з початковим. Як правило, перевірка здійснюється відразу після завантаження операційної системи — контролюються довжина файла, його контрольна сума, дата і час модифікації та інші параметри. Деякі програми-ревізори можуть при цьому виявляти і стелс-віруси. Гібриди програм-ревізорів і докторів можуть не тільки виявляти зміни, а й повертати файли і системні області до початкового стану. Вони є більш універсальними, оскільки можуть захистити і від вірусу, не відомого на час їх створення, якщо він використовує стандартний механізм зараження.

**Програми-фільтри («сторожа», «монітори») — резиденти}** програми, призначені для виявлення підозрілих дій при роботі комп'ютера. Після одержання відповідного повідомлення користувач може дозволити або відмінити виконання операції. Деякі програми-фільтри перевіряють програми, які викликаються до виконання, та файли, що копіюються. Недоліком подібних програм є їх «набридливість», можливі конфлікти з іншим програмним забезпеченням, а перевагами — виявлення вірусів на ранній стадії, що мінімізує втрати.

**Програми-вакцини («іммунізатори»)** модифікують програми і диски таким чином, що це не відбивається на роботі програм, але вірус, від якого проводиться вакцинація, вважає їх інфікованими. Це вкрай неефективний спосіб захисту. Вакцини мають обмежене використання — їх можна застосувати тільки проти відомих вірусів. Жодний з типів антивірусних програм не надає стовідсоткового захисту, тому слід додержувати загальних правил і користуватись останніми розробками антивірусних лабораторій.

# Методи криптографічного захисту

Криптографічний захист (шифрування) інформації - це вид захисту, який реалізується за допомогою перетворень інформації з використанням спеціальних (ключових) даних з метою приховування змісту інформації, підтвердження її справжності, цілісності, авторства тощо. На відміну від тайнопису, яке приховує сам факт передавання повідомлення, зашифровані повідомлення передаються відкрито, приховується їхній зміст. Методи криптографії поділяють на дві групи — підставлення (заміни) і переставлення.

Підстановчний метод передбачає, що кожна літера та цифра повідомлення замінюється за певним правилом на інший символ. Зокрема, для визначення порядку під- 15 ставлення може використовуватись певне слово або фраза — ключ. У загальному випадку у криптографії ключ — це послідовність бітів, що використовуються для шифрування та розшифрування даних.

У разі використання перестановного алгоритму змінюються не символи, а порядок їх розміщення в повідомленні. Залежно від доступності ключів розрізняють:

* **симетричне шифрування** — для шифрування і розшифрування використовується один ключ. Такі системи із закритим ключем реалізовані, наприклад, в архіваторах даних. Це зручно для шифрування приватної інформації, але під час передавання повідомлення по каналах зв'язку слід забезпечити таємне передавання ключа, щоб одержувач міг здійснити розшифрування. У принципі, якщо можна таємно передати ключ, то можна передати і таємну інформацію, тоді відпадає необхідність у шифруванні, а якщо такої можливості немає, шифрування даремне;
* **асиметричне** — для шифрування використовується один, відкритий (публічний, загальнодоступний) ключ, а для дешифрування — інший, закритий (секретний, приватний). Це робить непотрібним таємне передавання ключів між кореспондентами.

Відкритий ключ безплідний для дешифрування, і його знання не дає можливості визначити секретний ключ. Єдиним недоліком моделі є необхідність адміністративної роботи — ключі (і відкриті, і закриті) треба десь зберігати і час від часу оновлювати. Сьогодні існує достатня кількість криптографічних алгоритмів.

Ступінь захищеності під час використання цих алгоритмів прямо залежить від довжини ключа, що застосовується. Криптографічні алгоритми використовуються як для шифрування повідомлень, так і для створення електронних (цифрових) підписів (ЦП) — сукупностей даних, які дають змогу підтвердити цілісність електронного документа та ідентифікувати особу, що його підписала. Звичайно терміни «електронний підпис» і «цифровий підпис» застосовуються як синоніми, але перший з них має ширше значення, оскільки позначає будь-який підпис в електронній формі. Отже, електронні підписи не обов'язково базуються на криптографічних методах і можуть бути створені, наприклад, за допомогою засобів біометрії Цифровий підпис передбачає вставляння в повідомлення сторонньої зашифрованої інформації. Поширеним методом є створення ЦП за допомогою асиметричного шифрування.

При цьому накладання підпису виконується за допомогою закритого ключа, а перевірка підпису за допомогою відкритого (відмінність створення ЦП від шифрування інформації).

Публічний ключ та додаткові відомості (їм я відправника, серійний номер ЦП, назва уповноваженої фірми І ЦП) передається разом з підписом. Таким чином, послати зашифроване повідомлення і перевірити підпис може будь-хто, а розшифрувати або підписати повідомлення — тільки власник відповідного секретного ключа. Загалом для забезпечення належного рівня захищеності інформації потрібна криптографічна система (криптосистема) сукупність засобів криптографічного захисту, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (зокрема й такої, що визначає заходи безпеки). Головним обмеженням криптосистем є те, що при одержанні повідомлення зашифрованого парним ключем, не можна взнати напевне, хто саме його відправив. Останній недолік можна виправити за допомогоюо засобів біометричного захисту та методцом двофакторної аутентифікації. Наприклад, користувач повинен мати пластикову карті-ку (картку з магнітною смужкою або смарт-картку) і знати PIN-код. Отже, розвиток криптосистем і підвищення надійності цифрових підписів створює необхідні передумови для заміняй паперового документообігу електронним і переходу до здійснення електронних операцій.

# Технічні вимоги для проєкту

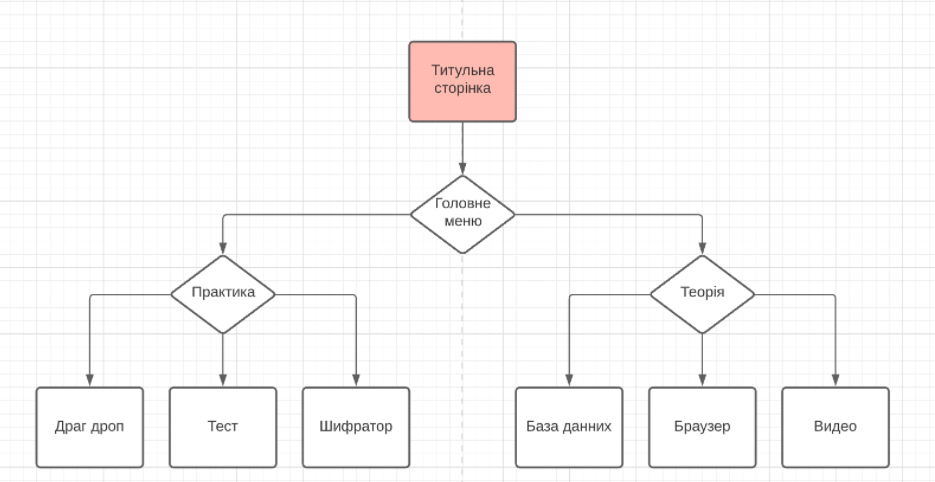
Для користування проектом на комп’ютері повинна бути встановлені

1) операційна система Windows 7 або пізніші версії;

2) Visual Studio 2019 або пізніші версії.

3) На жорсткому диску повинно бути вільні принаймні 5MB, та від 16 MB вільної оперативної пам’яті. Частота процесора повинна бути не менша від 2 GHz.

# Навігатор по проекту



# Посібник користувача

**Висновки**   
[Захист інформації](https://ua-referat.com/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97) є ключовим завданням у сучасних умовах взаємодії глобальних і корпоративних комп'ютерних мереж. У реальному світі багато уваги приділяється фізичної безпеки, а в світі електронного обміну інформацією необхідно піклуватися також про [засоби захисту даних](https://ua-referat.com/%D0%97%D0%B0%D1%81%D0%BE%D0%B1%D0%B8_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D0%B4%D0%B0%D0%BD%D0%B8%D1%85).  
Ускладнення методів і засобів організації машинної обробки, повсюдне використання глобальної мережі [Інтернет](https://ua-referat.com/%D0%86%D0%BD%D1%82%D0%B5%D1%80%D0%BD%D0%B5%D1%82) призводить до того, що інформація стає все оболе вразливою. Цьому сприяють такі чинники, як постійно зростаючі обсяги об'єми даних, накопичення і зберігання даних в обмежених місцях, постійне розширення кола користувачів, що мають доступ до ресурсів, програм і даних, недостатній рівень захисту апаратних і програмних засобів комп'ютерів і комунікаційних систем і т.п.  
Враховуючи ці факти, [захист інформації](https://ua-referat.com/%D0%97%D0%B0%D1%85%D0%B8%D1%81%D1%82_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97) в процесі її збору, зберігання, обробки і передачі набуває винятково важливого значення. У висновку хотілося б підкреслити, що ніякі апаратні, програмні і будь-які інші рішення не зможуть гарантувати абсолютну надійність і безпека даних у комп'ютерних мережах.  
У той же час звести ризик втрат до мінімуму можливо лише при комплексному підході до питань безпеки.

# Список використаної літератури [Інформатика](https://ua-referat.com/%D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%82%D0%B8%D0%BA%D0%B0) / Курносов А.П., Кульов С.А., Улезько А.В. та ін; під ред А.П. Курносова. - М.: Колос, 2005. Комп'ютерні мережі та [засоби захисту інформації](https://ua-referat.com/%D0%97%D0%B0%D1%81%D0%BE%D0%B1%D0%B8_%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97): Навчальний посібник / Камалян А.К., Кульов С.А., Назаренко К.М., Ломакін С.В., Кусмагамбетов С.М.; Під ред. д.е.н., професора А.К. Камалян. - [Воронеж](https://ua-referat.com/%D0%92%D0%BE%D1%80%D0%BE%D0%BD%D0%B5%D0%B6): ВДАУ, 2003. Леонтьєв В. П. Новітня енциклопедія персонального комп'ютера 2005. - М.: ОЛМА-ПРЕСС [Освіта](https://ua-referat.com/%D0%9E%D1%81%D0%B2%D1%96%D1%82%D0%B0), 2005.

# Черняков М.В., Петрушин А.С. [Основи інформаційних технологій](https://ua-referat.com/%D0%9E%D1%81%D0%BD%D0%BE%D0%B2%D0%B8_%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D0%B9). [Підручник](https://ua-referat.com/%D0%9F%D1%96%D0%B4%D1%80%D1%83%D1%87%D0%BD%D0%B8%D0%BA) для вузів: - М.: ИКЦ «Академкнига», 2007.

# Розділ 7 Cписок електронних джерел інформації

<https://neerc.ifmo.ru/wiki/index.php?title=%D0%94%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_%D0%BF%D0%BE_%D0%BF%D1%80%D0%BE%D1%84%D0%B8%D0%BB%D1%8E>

<https://wiki.algocode.ru/index.php?title=%D0%94%D0%9F_%D0%BF%D0%BE_%D0%BF%D1%80%D0%BE%D1%84%D0%B8%D0%BB%D1%8E>

<https://ru.wikipedia.org/wiki/%D0%94%D0%B8%D0%BD%D0%B0%D0%BC%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5>

<http://www.pereplet.ru/nauka/Soros/pdf/9802_139.pdf>

<https://habr.com/ru/post/191498/>

<https://e-maxx.ru/algo/profile_dynamics>

<https://ru.coursera.org/lecture/sportivnoe-programmirovanie/4-5-zadacha-parkiet-dinamika-po-profiliu-k3EYK>

<https://archive.lksh.ru/2011/july/B/files/dp-profile.pdf>