Національний університет «Пролтавська політехніка імені Юрія Кондратюка»

(повне найменування вищого навчального закладу)

Навчально-науковий інститут інформаційних технологій та робототехніки

(повна назва факультету)

Кафедра комп’ютерних та інформаційних технологій і систем

(повна назва кафедри)

**ПОЯСНЮВАЛЬНА ЗАПИСКА**

до кваліфікаційної роботи

*перший (бакалаврський)*

(рівень вищої освіти)

на тему: *Методика автоматизованого налаштування конфігурації безпеки мережевого обладнання на основі програмного забезпечення Аnsible*

Виконав: студент 4 курсу, групи 401-ТК

спеціальності

\_\_123 Комп’ютерна інженерія

(шифр і назва напряму)

Маладика Д.В.

(прізвище та ініціали)

Керівник \_\_\_\_\_\_\_Зінченко А.О.\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище та ініціали)

Рецензент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(прізвище та ініціали)

Полтава – 2021 року

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ  
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ « ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»**

**НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ  
ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ**

**КАФЕДРА КОМП’ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ**

**КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА  
спеціальність 123«Комп’ютерна інженерія» на тему**

**«Методика автоматизованого налаштування конфігурації безпеки мережевого обладнання на основі програмного забезпечення Аnsible»**

**Студента групи 401-ТК Маладики Дениса Вячеславовича**

Керівник роботи кандидат технічних наук, доцент Зінченко А.О.

Консультант

старший викладач

Черницька І.О.

Завідувач кафедри

кандидат технічних наук,

доцент Головко Г.В.

Полтава – 2021 року

# **АНОТАЦІЯ**

Кваліфікаційна робота: 63 сторінки.

Стрімке впровадження у життя особи, суспільства та держави сучасних інформаційних технологій призвело до створення інформаційного суспільства. Виробництво, засоби масової комунікації, повсякденна діяльність, все це зав’язано на сучасні інфокомунікаційні технології. Одночасно із різким збільшенням інформаційних сервісів збільшилася кількість сторонніх втручань в інформацінокомункаційні мережи різного призначення з метою заволодіння даними або спотворення інформації. Зазначене потребує удосконалення механізмів адекватної реакції у відповідь, необхідності використання засобі оркестрації для швидкого налаштування параметрів безпеки конфігурації мережевих пристроїв. Саме це визначило актуальність розробленої роботи бакалавра*.*

*Ключові слова*: кібербезпека, управління конфігурацією, оркестровка,

# ***ABSTRACT***

*Qualification work: 63 pages.*

*The rapid introduction of modern information technologies into the life of the individual, society and the state has led to the creation of the information society. Production, mass media, daily activities, all this is tied to modern infocommunication technologies. Simultaneously with the sharp increase in information services, the number of third-party interferences in information and communication networks for various purposes in order to capture data or distort information has increased.* *This requires the improvement of mechanisms for adequate response, the need to use the orchestration tool to quickly configure the security settings of network devices. This is what determined the relevance of the developed work of the bachelor.*

*Keywords: cybersecurity, configuration management, orchestration*

**ЗМІСТ**

[АНОТАЦІЯ 5](#_Toc75310276)

[ABSTRACT 6](#_Toc75310277)

[ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ 7](#_Toc75310278)

[ВСТУП 9](#_Toc75310279)

[РОЗДІЛ 1 АНАЛІЗ ІСНУЮЧИХ СУЧАСНИХ ЗАГРОЗ БЕЗПЕКИ МЕРЕЖЕВОГО ОБЛАДНАННЯ 10](#_Toc75310280)

[1.1 Стан інформаційної безпеки в Україні 10](#_Toc75310281)

[1.2 Кібербезпека у сучасних умовах 13](#_Toc75310282)

[1.3 Необхідність захисту даних і мереж 17](#_Toc75310283)

[1.4 Наслідки порушення безпеки 23](#_Toc75310284)

[1.5. Види загроз для користувачів, їх властивості та типи кібератак 29](#_Toc75310285)

[Висновки до першого розділу 44](#_Toc75310286)

[РОЗДІЛ 2 МЕТОДИ АВТОМАТИЗОВАНОГО НАЛАШТУВАННЯ КОНФІГУРАЦІЙ БЕЗПЕКИ МЕРЕЖЕВОГО ОБЛАДНАННЯ 46](#_Toc75310287)

[2.1. Сучасні методи оркестрації та управління конфігурацією 46](#_Toc75310288)

[2.2. Порівняння Ansible, Chef, Puppet та SaltStack 51](#_Toc75310289)

[Висновки до другого розділу 57](#_Toc75310290)

[РОЗДІЛ 3 МОДЕЛЬ АВТОМАТИЗОВАНОГО НАЛАШТУВАННЯ КОНФІГУРАЦІЇ БЕЗПЕКИ МЕРЕЖЕВОГО ОБЛАДНАННЯ НА ОСНОВІ ПЗ ANSIBLE 58](#_Toc75310291)

[3.1 Модулі для роботи з мережевим обладнання 58](#_Toc75310292)

[Висновки до третього розділу 61](#_Toc75310293)

[ВИСНОВКИ 62](#_Toc75310294)

[СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 64](#_Toc75310295)

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ І ТЕРМІНІВ**

API (*Application Programming Interface) –* прикладний програмний інтерфейс

IaaS (*Infrastructure as a Service)* – інфраструктура як сервіс

IT (*Information Technology) –* інформаційні технології

JSON *(JavaScript Object Notation) –* запис об’єктів JavaScript

ПЗ – програмне забезпечення

SSH (*Secure Shell) –* протокол віддаленого доступу

SSL *(Secure Sockets Layer) –* рівень захищених токенів

YAML *(Yet Another Markup Language) –* мова розмітки

ID (*Identit Document*) – ідентифікатор

*ISO* (*International Standards Organiz*ation) –міжнародна організація зі стандартизації

MAC (*Media Access Control) –* управління доступом

MD5 (*Message Digest* 5) – 28-бітний алгоритм хешування

**ВСТУП**

**Актуальність дослідження.** Сучасні загрози національній безпеці України не обмежуються лише силовим протистоянням. На теперішній час особливої ваги набуває проблема інформаційної безпеки. Це доводить досвід більшості країн світу та реалії сьогодення. Аналіз останніх події в Україні свідчить про реалізацію сценарію гібридної війни із ключовою роллю інформаційного впливу. За таких умов набувають актуальності питання посилення структур інформаційної безпеки України, здатних протистояти масованому інформаційному впливу з боку противника. Важливою складовою інформаційної безпеки є кібербезпека, а саме безпека мереж та даних. Тому актуальним є завдання, що полягає в удосконаленні налаштування конфігурації безпеки мережевого обладнання

**Метою дослідження** підвищити рівень безпеки шляхом розроблення моделі автоматизованого налаштування параметрів безпеки на мережевому обладнанні.

**Об’єктом дослідження** є процес автоматизованого налаштування конфігурації безпеки мережевого обладнанні.

**Предметом дослідження** є програмне забезпечення управління конфігурацією мережі.

**Для досягнення мети дослідження необхідно виконати наступні часткові завдання дослідження**:

провести аналіз існуючих сучасних загроз безпеки мережевого обладнання;

провести аналіз додатків автоматизованого налаштування безпеки мережі;

розробити модель автоматизованого налаштування конфігурації безпеки мережевого обладнання на основі програмного забезпечення Ansible.

**РОЗДІЛ** **1  
АНАЛІЗ ІСНУЮЧИХ СУЧАСНИХ ЗАГРОЗ БЕЗПЕКИ МЕРЕЖЕВОГО ОБЛАДНАННЯ**

* 1. **Стан інформаційної безпеки в Україні**

За поглядами провідних вчених України інформаційна безпека (ІБ) – це інтегральна сукупність різних заходів органів держаної влади в інформаційній сфері, що мають на меті захист національної безпеки та оборони України [1-3].

Під цим мається на увазі, що заходи негативного інформаційного впливу, у тому числі і у кіберпросторі не завдають збітків національним інтересам України.

У відповідності із законодавчою базою України існують наступні рівні забезпечення інформаційної безпеки. Рівень особистості, рівень громадянського суспільства, рівень держави.

У [Доктрині](https://uk.wikipedia.org/wiki/Доктрина) інформаційної безпеки України, що введена у дію Указом президента України від 25 лютого 2017 року № 47/2017, визначено серед загроз інформаційній безпеці країни:

здійснення інформаційних операцій, що мають за мету деморалізацію особового складу сектору безпеки і оброни України, провокування екстремізму, поширення паніки серед цивільного населення України;

розпалювання міжнаціональної, міжконфесійної ворожнечі;

проведення агресором інформаційних операцій щодо створення негативного іміджу України;

недостатня розвиненість в України сучасної інформаційної інфраструктури.

Тому важливого значення набуває питання оцінювання рівня інформаційної безпеки. Визначення показників та критеріїв для проведення комплексного оцінювання рівня інформаційної безпеки є методологічною основою стосовно визначення вимог щодо захисту комп'ютерних систем кібервпливу, створення комплексних систем захисту інформації і проведення інформаційного аудиту.

Визначені критерії оцінювання надають можливість провести порівняння різних методик захисту інформації та визначити найбільш оптимальну стратегію захисту інформації у комп’ютерних системах [3, 4].

З урахуванням комплексного характеру захисту інформації для оцінювання її рівня використовують модель тріади *CIA*. Вона передбачає у якості часткових показників інформаційної безпеки використання конфіденційності, цілісності, доступності.

Існуючі інформаційні системи стосовно інформаційної безпеки оцінюються за трьома напрямками. Це технічні засоби, програмне забезпечення і комунікації. Наведений підхід є основою використання існуючих стандартів у галузі інформаційної безпеки. При цьому стандарти застосовуються на фізичному, особистому та організаційному рівнях. Іншими словами існуючі стандарти інформаційної безпеки реалізуються для адміністраторів, користувачів та операторів мереж з метою упорядкування правил використання захисних процедур для гарантування інформаційної безпеки.

Під безпекою мережі розуміється комплекс заходів, що спрямований на захист мережі від: [несанкціонованого доступу](https://uk.wikipedia.org/wiki/Несанкціонований_доступ), випадкового (навмисного) втручання у функціонування мережі, спроб руйнування компонентів мережі, знищення або спотворення інформації, що знаходиться у мережі [3, 4].

Складовими системи безпеки інформаційної мережі є захист мережевого обладнання, спеціалізованого програмного забезпечення, даних і персоналу (операторів, користувачів). Безпека мережі спрямовується на запобігання несанкціонованому доступу до мережі та інформації, неправильному використанню, зміні (відмові) у доступі до комп'ютерної мережі або до мережевих ресурсів. Вона складається з правил, положень і політики, що встановлюється адміністратором комп’ютерної мережі. Одне із правил це надання адміністратором дозволу на доступ до даних мережі. Для перевірки правильності доступу до мережі та її ресурсів використовується призначені користувачам *ID*, паролі або інші методи перевірки автентичності інформації і користувачів.

Політики мережевої безпека встановлюється для всіх типів мереж. Вони забезпечують безпеку інформації під час здійснення взаємодії між приватними, державними комп'ютерні мережами, мережами організацій, установ і приватних осіб. Самим поширеним методом захисту мережевих ресурсів є присвоєння кожній мережі, операторам і користувачам індивідуального ім’я або паролю [5].

Аутентифікації користувача у мережі зазвичай включає у себе перевірку ім'я користувача та його пароля. Випадок, коли політикою безпеки для аутентифікації користувача потрібно тільки ім'я користувача, має назву однофакторна аутентифікація. Для проходження двофакторної аутентифікації потрібно підтвердження особи користувача ще за одним елементом. Після встановлення особи брандмауер комп’ютерної системи забезпечує доступ користувачам до ресурсів мережі.

З метою виявлення і нейтралізації негативного впливу шкідливих програм (вірусів) застосовується спеціалізоване антивірусне програмне забезпечення або комплексні системи запобігання несанкціонованих вторгнень у мережу.

Для забезпечення конфіденційності обміну даними між комп’ютерами у мережі можливо застосування процедури шифрування даних.

Комплексні системи захисту інформації у комп’ютерній мережі не обмежуються використанням одного методу. Застосовується цілий комплекс засобів захисту. Такий підхід приводить до того, що відключення частини обладнання не впливає на продовження функціонування системи захисту. Решта мережевого обладнання продовжує захищати дані мережі від несанкціонованого доступу.

Наявність доступу до ресурсів мережі Інтернет за умови правильного встановлення політики рівнів безпеки комп’ютерної мережі надає можливість користувачу цілодобового доступу до інформації.

**1.2 Кібербезпека у сучасних умовах**

Важливе значення для ведення воєнних дій сьогодення має кіберпростір. Бойові дії у кіберпросторі можуть вестися без традиційного зіткнення військ на полі бою. Проте ефективність застосування сил та засобів саме у кіберпросторі не викликає сумнівів. Це дозволяє країнам з не великими військовими силами за рахунок ведення асиметричних дій впевнено діяти у відповідь на агресивні дії більш потужного противника [6-8].

Сталого визначення кібервійна не існує. Тому наведемо власне бачення. Кібервійна – це зіткнення противників у кіберпросторі для досягнення своїх національних інтересів з використанням сучасних інформаційних технологій. Таким чином кожна сторона конфлікту буде використовувати сучасні інформаційні технології, спеціально навчений особовий склад для нанесення збитків іншій стороні у різних сферах діяльності. Наприклад, порушення роботи банківського сектору [6-8].

Яскравим прикладом такого втручання у роботу комп’ютерних мереж було застосування комп’ютерного вірусу Stuxnet. Цілю атаки було виведення з ладу фабрики зі збагачення урану і взагалі зрив ядерної програми Ірану. Особливістю бойового застосування комп’ютерного вірусу була бездоказовість атаки, тобто не можливість встановити противника. Stuxnet зламав комп’ютери, що управляли виробництвом, з метою пошкодити цінне фізичне обладнання, що управлялося цими комп'ютерами.

На підставі наведеного прикладу можливо встановити основну мету кібервійни. Це отримати перевагу над противниками, незалежно від того, чи є вони державами або конкурентами.

Держава може постійно втручатися в інфраструктуру іншої країни, викрадати військові секрети та збирати інформацію про технології, щоб скоротити відставання у своїх галузях промисловості та військовій сфері. Окрім промислового та військового шпигунства, під час кібервійни можуть здійснюватися диверсії на інфраструктуру інших країн і це може коштувати людських життів в країнах-цілях. Наприклад, атака може зруйнувати енергосистему великого міста. Дорожній рух буде порушено. Обмін товарами та послугами зупинено. Пацієнти не зможуть отримати необхідну допомогу в надзвичайних ситуаціях. Доступ до Інтернету також може бути порушеним. Зачепивши енергосистему, напад може вплинути на повсякденне життя простих громадян [6-8].

Крім того, скомпрометовані конфіденційні дані надають нападникам можливість шантажу персоналу в уряді. Інформація може дозволити зловмиснику видати себе за авторизованого користувача для доступу до конфіденційної інформації або обладнання.

Якщо уряд не може захистити громадян від кібератак, то вони можуть втратити довіру до здатності уряду захищати їх. Кібервійна може дестабілізувати державу, зруйнувати торгівлю та впливати на довіру громадян у їхній уряд, навіть коли немає фізичного вторгнення в країну-жертву.

Можливо ввести класифікацію кібервійн. Основними будуть наступальна і захисна кібервійна (кібердії). Основним змістом кібервійн буде ведення кібероборони держави, кібероперацій (наступальні, обороні), розгортання додаткової інфраструктури у кіберпросторі, кіберзахист, кібератаки, кібернапад, кіберрозвідка [6-8].

Можливо також класифікувати кібердій. Це будуть дії у кіберпросторі та дії через кіберпростір. Яскравим прикладом дій через кіберпростір є досягнення мети через використання кіберпростору. Наприклад, вандалізм (зміна змісту інформації, паплюження, нанесення образи); ведення пропаганди (розсилка повідомлень, реклама); збір інформації (зламування профілів, приватних сторінок, серверів, збір інформації обмеженого користування); відмова у наданні сервісу; втручання у функціонування технологічного устаткування; кібератаки на об'єкти критичної інфраструктури (атомна енергетика, гідроспоруди, теплоенергетика, рух повітряного і наземного транспорту та інше).

За поглядами деяких дослідників (див. Мікко Хіппонен з фірми F-Secure) початком кібервійни між Україною і Російською Федерацією можливо вважати кібератаку на енергетичний сектор у вересні 2015 року. Метою було не збір інформації обмеженого користування, крадіжка грошей чи щось інше. А саме нанесення великих втрат енергетичному сектору України. У подальшому було застосування сумнозвісного вірусу *Pety* і його римейку *NewPety*.

Стрімке поширення інформаційних технологій у наше сьогодення призвело до значної залежності громадян, підприємств і державних установ він наявності інтернет доступу до мережі. Використання кіберпростору для завдання кібератак на інформаційну інфраструктуру держави може дестабілізувати обстановку в окремій країні. Провідними країнами світу саме кібервійна вважається однією із основних загроз безпеці держави [9-11].

Розвідки багатьох країн також активно використовують інтернет для збору розвідувальної інформації. За поглядами фахівців лідерами з питань кіберрозвідки є [Китай](https://uk.wikipedia.org/wiki/Китай) та [Росія](https://uk.wikipedia.org/wiki/Росія). Китай часто звинувачують в організації проведення систематичних кібератак на сайти державних установ Сполучених Штатів Америки, [Німеччини](https://uk.wikipedia.org/wiki/Німеччина), [Індії](https://uk.wikipedia.org/wiki/Індія). Російська Федерація систематично проводить кібератаки на недружні країни. Серед них Україна, Сполучені Штати Америки, Литва, Латвія, Польща, Чехія. Однак, принцип бездоказовості, що існує у кіберпросторі, вимагає прикладення значних зусиль для аргументованого доведення таких фактів.

Не осталися осторонь від питань ведення кібервійн і неформальні угруповання українських хакерів. Так, у відповідь на акт вандалізму на горі Говерла, невідомим неформальним угрупованням українських хакерів були атаковані сайти Євразійського союзу молоді (РФ), що взяв на себе відповідальність за факт вандалізму.

Розвиток нових інформаційних технологій призводить до постійного вдосконалення змісту кібервійн. Провідні держави світу приступили до формування та набуття спроможностей військові частини та підрозділи кібербезпеки. Удосконалюється їх технічне оснащення і навченість.

З початком “гібрідної” війни у 2014 році між україною та Російською Федерацією інформаційнокомунікаційні мережі України не одноразово ставали обєктами нападу у кіберпросторі з боку РФ. При цьому участь у проведенні кібератак брали як штатні підрозділи Збройних Сил РФ так і неформальні угруповання хакерів РФ. Так у 2014 році під час проведення виборів Президента України фахівцями СБУ за напрямком кібербезпеки спільно з *CERT*-*UA* ДСЗЗІ було нейтралізовано проведення кібер атак на інформаційно-аналітичну систему Центральгнної виборчої комісії України. Відповідальність за проведення кібератаки взяло неформальне російське обєднання *Cyber*-*Berkut*. Також за даними розвідки було встановлено, що додатково була залучена до проведення кібератаки група АРТ-28 із вірусом під назвою *SOFACY* [12].

Робота щодо відновлення пошкодженої системи тривала декілька днів. Були залучені фахівці компанії Датагруп. З метою надання удару у відповідь та доказів про причетність РФ фахівці з кібербезпеки СБУ встановили логічну пастку для ворога. Ця пастка відпрацювала на всі 100 відсотків. Противником була одержано не правдиву інформацію про перемогу на виборах Президента України Дмитра Яроша. 25 травня 2014 року більшість російських пропагандистських каналів оприлюднило цю новину. Одночасно фахіцями з кібербезпеки СБУ було зафіксовано входження до інформаціно-аналітичної системи ЦВК з *IP*-адреси, що входить переліку адрес телеканалу [ОРТ](https://uk.wikipedia.org/wiki/ОРТ)[.](https://uk.wikipedia.org/wiki/Кібервійна#cite_note-14)

Всього в Україні з початку 2014 року у середньому фіксується до 1,5 тисяч кібератак на інформаційний простір україни з боку РФ.

23 грудня 2015 року була зафіксована успуішна кібератака на інформаціно-управляючу систему [«Прикарпаттяобленерго»](https://uk.wikipedia.org/wiki/Прикарпаттяобленерго). Атака була проведена з ІР адрес РФ використанням шкідливого програмного забезпечення BlackEnergy. Результатом стало вимкнення електроживлення на території Львівської області на протязі шести годин.

Для реагування у відповідь на виклики з боку РФ 16 березня 2016 року Президентом України Петром Порошенком було введено у дію рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Стратегією передбачено формуваня в Україні комплексної системи забезпечення кібербезпеки України. Було визначено склад, завдання, принципи формування системи забезпечення кібербезпеки України. Визначенні субєкти та обєкти кібербезпеки. Проведено розподіл відповідальності між субєктами забезпечення кібернетичної безпеки України.

Для деталізації та впровадження положень наведеної Стратегії було розроблено та прийнято Закон України “Про основні засади забезпечення кібербезпеки України” від 5 жовтня 2017 року № 2163-VIII. Закном було визначено правові та організаційні основи забезпечення житєво важливих інтересів у кіберпросторі України.

**1.3 Необхідність захисту даних і мереж**

Доступ до ресурсів інформаційно-телекомуніукаційної мережі Інтернет став необхідною умовою нашого сьогодення. Для забезпечення успішного функціонуваання всі організації та установи не залежно від форми власності використовують мережі передачці даних (Інтернет). Ресурси мережі застосовуються для збору, обробки, зберігання та обміну необхідною для роботи інформацією у цифровому вигляді. Тому захист наведеної інофрмації стає житево необхідним для забезпечення сталого функціонування національної економіки і національної безпеки [6, 13, 14].

Для забезпечення безпеки і добробуту гррмадян на рівні особистості потребують захисту персональні данні, паролі та персональні електронні обчисювальні машини. На рівні організації відповідальність персоналу зосереджується на підтримані репутації організації, захисті даних організації і персональних даних клієнтів. На рівні держави для забезпечення вихзначеного рівня національної безпеки захисту підлягає інформації з обмеженим доступом, важлива для національної безпеки держави. Саме на забезпечення визначених завдань на всіх рівнях спрямовуються зусилля системи забезпечення кібернетичної безпеки.

Друзі з якими ви спілкуєтьися, колеги по роботі, однокласники і сокурсники, члени родини знають дуже багато інформації про вас. Призвище та імя, адреса мешкання, паспортні дання, індивідуальний код, освіта, сімейний стан. Ця інформація знайшла назву офлайн ідентичності особи. Онлайн ідентичність – це той набір даних про себе, що надаєте при спілкування у кіберпросторі (Інтернеті). Візьмість за правило обмежувати кількість інформації про себе у кіберпросторі. Люба інформація про вас може бути використанна про вас. І чим більше ви будете знаходитися у кіберпромсторі тим більше у зловмисників буде можлиивості ідентифікувати вашу особистість.

Імя користувача інтернету (псевдонім) для сворення профілю в Інтернеті не повино бути повязано з персональною інформацією. Імя в інтернеті не повино провокувати увагу кіберзлочинців на здійснення негативних дій щодо вас. Воно повино нести нейтральний характер і бути ввічливим і доречним.

Візміть за правило, що люба інформація про вашу особистість повина бути приватною інформацією. Наведена інформація надає змогу вас індентифікувати. Це ваші фотографії, переписка спілкування у соціальних месенджирах. Вони дають змогу шахраям встановити ваше імя, паспортні дані, індивідуальний код, дату та місце народження. Доречі, відомості про місце роботи, медичне забезпечення, освітну, банківську інформацію також можуть слугувати для зловмисників допомогою при вашій індентифікації в Інтернеті.

Кожного разу, коли ви відвідуєте кабінет лікаря, до ваших електронних медичних записів (*Electronic Health Records*, *EHR*) додається більше інформації. Виписка від вашого сімейного лікаря стане частиною вашого *ЕHR*. Ваш *EHR* включає в себе інформацію про ваше фізичне і психічне здоров'я та інші особисті дані, які можуть бути не пов'язані з медичними проблемами. Наприклад, якщо ви мали в дитинстві консультації психолога, коли відбувалися серйозні зміни у сім'ї, це буде десь відображено у ваших медичних записах. Окрім вашої медичної історії та особистої інформації, *EHR* також може містити інформацію про вашу сім'ю.

Медичні пристрої, такі як фітнес-доріжка, використовують хмарну платформу, щоб забезпечити можливість бездротового передавання, зберігання та відображення клінічних даних, таких як частота серцевих скорочень, артеріальний тиск та рівень цукру в крові. Ці пристрої можуть генерувати величезну кількість клінічних даних, які можуть стати частиною ваших медичних записів.

Коли ви здобуваєте свою освіту, інформація про ваші оцінки та тестові результати, відвідування занять,курси, нагороди та присвоєні ступені, а також будь-які записи про дисциплінарні порушення можуть бути відображені у цих записах. Ці записи також можуть містити контактну інформацію, записи про стан здоров'я та вакцинації, а також записи про спеціальну освіту, індивідуальні освітні програми (*Individualized Education Programs*, *ІЕР*).

Ваші фінансові записи можуть містити інформацію про ваші доходи та витрати. Податкові записи можуть містити інформацію про заробітну плату, номери банківських карт, ваш кредитний рейтинг та іншу банківську інформацію. Ваша інформація про зайнятість може включати відомості про вашу попередню та теперішню роботу.

Все наведене це ваші особисті дані. Існують різні закони, які захищають вашу конфіденційність та дані у вашій країні. Але чи знаєте ви, де саме знаходяться ваші дані?

Коли ви перебуваєте в кабінеті лікаря, ця розмова записується до вашої медичної картки. Для покриття страхових витрат ці відомості можуть надсилатись у страхову компанію, щоб забезпечити відповідну оплату та якість послуг. Тепер частина ваших медичних записів, які стосуються цього візиту, також зберігаються у страховій компанії.

Картки лояльності магазинів можуть бути зручним способом заощадити кошти на покупках. Однак, магазин складає профіль ваших покупок і використовує цю інформацію для власних цілей. У профілі показано, що покупець регулярно купує зубну пасту певної марки та типу. Магазин використовує цю інформацію, щоб націлити покупця на спеціальні пропозиції від маркетингового партнера. Використовуючи картку лояльності, магазин та маркетинговий партнер отримують профілі покупців для передбачення поведінки клієнтів.

Коли ви ділитесь своїми фотографіями в Інтернеті з друзями, чи знаєте, хто може одержати копії фотографій? Копії фотографій містяться на ваших власних пристроях. Ваші друзі можуть мати копії фотографій, завантажених на їхні пристрої. Якщо фотографії публікуються, як загальнодоступні, незнайомці також можуть мати їх копії. Вони можуть завантажувати ці фотографії або робити скріншоти з цих фотографій. Оскільки зображення були розміщені в мережі, вони також зберігаються на серверах, розташованих у різних частинах світу. Тепер ці фотографії можна знайти не лише на ваших електронних пристроях.

Наші електроні помічники зберігають наші особисті, персональні дані. Одночасно вони стали джерелом поширення цієї особистої інформації.

На випадок вашої відмови від зберігання персональних даних на паперових носіях іпереходу до цифрової форми використовуйте для доступу до неї тільки свої електроні засоби доступу до неї. Інакше ваші персональні данні стануть відомі шахраям та хакерам. Особливо оборежними потрібно буди з персональними даними фінансового характеру.

Якщо у вас є що-небудь цінне, злочинці захочуть це викрасти. Ваші онлайн персональні відомості є надзвичайно коштовними для шахраїв. Вони дають доступ шахраям до виших банківсських рахунків.

Можливо, ви думаєте, що преміальні милі авіакомпаній, які ви заробили, не є цінними для кіберзлочинців. Подумайте ще раз. Після того, як були зламані близько 10 000 облікових записів авіакомпаній *American* *Airlines* та *United* *Airlines*, кіберзлочинці заброньовали безкоштовні перельоти, використовуючи ці викрадені облікові дані. Навіть, незважаючи на те, що, милі були повернуті клієнтам авіакомпаній, це демонструє цінність облікових даних.

Шахраї можуть встановити членів вашої родини та скористатися цім. За різними шахрайськими схемами вони будуть пробувати отримати дані ваших і членів вашої родини облікових записів. Пробувати під різними приводами, щоб ви перерахували кошти вашим близьким та родичам. Широкого розповсюдження набуло відправлення повідмлень та телефоні дзвінки про необхіднсть термінової фінансової допомоги для виших рідних, коли вони у біді.

Кіберзлочинці мають бурну фантазію яку спрямовують на пошук нових способів ошукати вас. Вони прагнуть вкрасти не тільки гроші а і ваше життя. Метою їх дій є не тільки крадіжка ваших грошей. Тому що викравши ваш профіль у кіберпрорсторі вони зможуть довго видавати себе за вас і робити крадіжки систематично. Оскільки медичні витрати зростають, крадіжки медичних страхових полісів також частішають. Злочинець може викрасти ваш медичний страховий поліс та використатися вашим медичним обслуговування для себе. Пройдені злочинцем медичні процедури відобразяться у ваших медичних документах.

Щорічні процедури подання податкової декларації можуть відрізнятися у залежності від країни, проте кіберзлочинці розглядають цей час як нові можливості. Наприклад, у Сполучених Штатах потрібно подати свої податкові декларації до 15 квітня кожного року. Податкове управління (*The* *Internal* *Revenue* *Service*, *IRS*) не перевіряє податкову декларацію та інформацію від роботодавця до липня. Зловмисник може подати підроблену податкову декларацію та одержати відшкодування. Реальні декларанти помітять це, коли їхні декларації про доходи будуть повернені податковою. За допомогою викраденої ідентичності вашої особи кіберзлочинці відкривають фіктивні рахукнки та беруть кредити на ваше ім'я. Це спричинить шкоду вашій репутації та зашкодить вашим подальшим взаємовідносинам з банківськими установами. Крадіжка особистого профілю може надати крадіям доступ до закритих даних організації, або взагалі до матеріалів що містять інформацію з обмеженим доступом.

Дані про організацію містять у собі інформацію про роботодавців та найманих працівників, нові інтелектуальні рішення і фінансову звітність організації. Інформацію про роботодавців та найманих працівників може включати заяви робітників, лікарняні листи, відомості про нарахування заробітної платні, скарги, завяви, пропозиції, типові контракти робітників та та будь-яка інша інформація стсовно персоналу компанії. Відомості про нові інтелектуальні рішення (патенти, корисні моделі, технолгічні рішення та інше) є критичними для існуваання підприємства. Вони дозволяють мати економічну перевагу у конкурентному середовищі. Фінансова завітність компанії може дати уявлення про реальний стан підприємства та використана конкурентами та іншими доброзичливцями не на користь підприємства.

Наступноим важливим кроком на шляху розвитку інформаційних технолшлгій стала поява Інтернету речей (*Internet of Things*). Одночасно зросли у ризики у напрямку кібербезпеки. Інтернет речей – це велика мережа фізичних об'єктів, що підєднуються до комп'ютерної мережі. Такий підхід різко збільшує кількість даних, що циркулює у середині такої мережі. Через це використовуються хмарні технології (*Cloud* 0) і технолгії віртуалізації. Обєм ціфрових даних зростає за експотенціальним законом. Наведене спонукало до стрімкого розвитку окремого ррозділу інформаційних технологій – великих баз даних (*Big* *Data*). Це спонукає користувачів та системних адміністраторів мереж ще більш відповідально підійти до питань безпеки даних (кібербезпеки).

**1.4 Наслідки порушення безпеки**

Захистити організацію від будь-якої можливої кібератаки неможливо з кількох причин. Експертна оцінка, що необхідна для налаштування та підтримки безпеки мережі, може мати високу вартість. Зловмисники завжди будуть шукати нові способи атак на мережі. Тож просунута та цілеспрямована кібератака буде успішною. У такому вирадку, пріоритетним буде те, наскільки швидко ваша команда безпеки може зреагувати на атаку, щоб мінімізувати втрати даних, час простою та втрати прибутку [6, 15, 16].

Як ви вже знаєте, будь що розміщене в Інтернеті може залишатись там назавжди, навіть якщо ви змогли стерти всі копії, що є у вашому розпорядженні. Якщо ваші сервери були зламані, конфіденційна інформація про персонал може бути оприлюднена. Хакер або група хакерів має змогу нанести шкоду веб-сайту організації компанії. Вони можуть внести на сайт викривлену, спотворену інформацію чим невелювати репутацію організації. Вони зможуть взагалі знищити сайт організації чи компанії. Це униможливить нормальне функціонування та призведе до фінансових втрат. Злом хакерами сайту або інфокомунікаційної мережі компанії може призвести до витоку документів з обмеженим доступом і сприяти падінню рейтингової репутації та акцій компанії [6, 15, 16].

Грошова вартість збитків набагато вища, ніж просто заміна будь-яких втрачених або викрадених пристроїв, інвестування в існуючу безпеку та зміцнення фізичної безпеки будівлі. Компанія повинна повідомити про злам клієнтів, на яких це може вплинути, та бути готовою до судових позовів. Через усі ці потрясіння співробітники можуть звільнитись з компанії. Компанії, можливо, буде потрібно більше зосередитись на відновленні своєї репутації, а не на зростанні.

Інтернет-менеджер паролів *LastPass* виявив незвичну активність у своїй мережі в липні 2015 року. Виявилося, що хакери викрали електронні адреси користувачів, нагадування про зміни паролів та хеші аутентифікації. На щастя для користувачів, хакери не змогли отримати доступ до сховищ зашифрованих паролів.

Навіть незважаючи на порушення безпеки, *LastPass* все ще може захистити інформацію облікових записів користувачів. *LastPass* вимагає перевірки електронної пошти або багатофакторної аутентифікації, коли з'являється новий логін з невідомого пристрою або невідомої *IP*-адреси. Хакерам також потрібно мати майстер-пароль для доступу до облікового запису.

Користувачі *LastPass* також несуть певну відповідальність за захист своїх власних облікових записів. Користувачі повинні завжди використовувати складні майстер-паролі та періодично їх змінювати. Користувачі завжди мають остерігатися фішингових атак. Прикладом атаки з фішингу може бути ситуація, коли зловмисник надсилає підроблені електронні листи, у яких вказується, що вони надіслані з *LastPass*. Електронні листи закликають користувачів натиснути на вбудоване посилання та змінити пароль. Посилання в електронному листі переадресовує на шахрайську версію веб-сайту, що використовується для викрадення майстер-пароля. Користувачі ніколи не повинні натискати вбудовані посилання в електронному листі. Користувачі також повинні бути обережні з відновленням пароля. Відновлення паролю не повинно повертати ваші паролі. Найголовніше це те, що користувачі повинні вмикати багатофакторну автентифікацію, коли це доступно для будь-якого веб-сайту, який це пропонує.

Якщо користувачі та постачальники послуг використовують належні інструменти та процедури для захисту інформації користувачів, дані користувачів все ще можуть бути захищені, навіть у випадку порушення безпеки.

Високотехнологічний виробник дитячих товарів *Vtech*, зазнав порушення системи безпеки своєї бази даних в листопаді 2015 року. Це порушення могло вплинути на мільйони клієнтів у всьому світі, включаючи дітей. Злам даних розкрив конфіденційну інформацію, включаючи імена клієнтів, адреси електронної пошти, паролі, фотографії та історії чату.

Новою ціллю для хакерів став ігровий планшет. Клієнти ділилися фотографіями та використовували функції чату з ігрових планшетів. Інформація не була належним чином захищена, а веб-сайт компанії не підтримував безпечне *SSL*-з'єднання. Навіть незважаючи на те, що "дірка" в системі безпеки не містила жодної інформації про кредитні картки та особисті ідентифікаційні дані, компанія була відсторонена на фондовій біржі, настільки великим було занепокоєння з приводу хакерського втручання.

*Vtech* захищав інформацію про клієнтів не належним чином, що виявилось під час проникнення. Навіть незважаючи на те, що компанія інформувала своїх клієнтів про те, що їх паролі хешовані, хакери все ж могли розшифрувати їх. Паролі в базі даних були хешовані за допомогою хеш-функції *MD5*, але секретні питання та відповіді на них зберігалися у звичайному тексті. На жаль, функція хешування *MD5* має відомі вразливості. Хакери можуть визначити оригінальні паролі, порівнюючи мільйони попередньо розрахованих значень хешу.

Інформацію, розкриту під час цього зламу, кіберзлочинці могли використовувати для створення облікових записів електронної пошти, подання заявок на отримання кредитів та вчинення інших злочинів, перш ніж діти стануть достатньо дорослими, щоб піти у школу. Батьки цих дітей також потенційно постраждали, оскільки кібер-злочинці могли використовувати їх онлайн-рахунки, оскільки багато людей повторно використовують свої паролі на різних веб-сайтах і в облікових записах. Порушення безпеки не лише вплинуло на конфіденційність споживачів, але й знищило репутацію компанії, коли її усунули з фондової біржі.

Для батьків, це попередження бути пильними та дбати про конфіденційність своїх дітей в Інтернеті та вимагати кращої безпеки для дитячих товарів. Виробники товарів, що пов'язані з мережею, повинні бути більш активними у захисті даних клієнтів та конфіденційності, як зараз так і в майбутньому, оскільки ландшафт кіберзагроз еволюціонує.

Нападники – це особи або групи, які намагаються використати кібер-вразливість для особистої або фінансової вигоди. Вони зацікавлені у всьому, від кредитних карток до дизайну продукту та будь чого, що має цінність.

Аматори – цих людей іноді називають скріпт-дітьми. Як правило, це зловмисники, які практично не мають навичок і часто для запуску атак використовують існуючі інструменти або знайдені в Інтернеті інструкції. Деякі з них роблять це просто з цікавості, а інші намагаються продемонструвати свою майстерність і завдати шкоди. Вони можуть використовувати базові інструменти, але результати можуть бути руйнівними.

Хакери – ця група зловмисників, що з метою отримати доступ зламують комп'ютери або мережі,. Залежно від наміру вторгнення ці зловмисники класифікуються як Білі, Сірі або Чорні капелюхи. Білі капюлюхи втручаються в мережі або комп'ютерні системи, щоб виявити слабкі місця та покращити безпеку цих систем. Ці вторгнення виконуються за попереднім дозволом і всі результати повідомляються власнику.

З іншого боку, Чорні капелюхи використовують будь-яку вразливість для незаконної особистої, фінансової або політичної користі. Сірі капелюхи знаходяться десь посередині між Білими та Чорними. Сірі капелюхи можуть виявити вразливість у системі. Та можуть повідомити про вразливість власників системи, якщо це збігається з їхніми планами. Деякі Сірі капелюхи публікують факти про вразливість в Інтернеті, щоб інші нападники могли їх використовувати.

Організовані хакери – до таких хакерів відносяться організації кіберзлочинців, хактивісти, терористи та хакери, що фінансуються державою. Кіберзлочинці зазвичай є групами професійних злочинців, орієнтованих на контроль, владу та багатство. Ці злочинці дуже витончені та організовані і вони навіть можуть надавати кіберзлочинність, як сервіс іншим злочинцям.

Хактивісти роблять політичні заяви, щоб проінформувати про важливі для них питання. Нападники, які фінансуються державою, здійснюють розвідку чи саботаж від імені свого уряду. Ці нападники, як правило, якісно підготовлені та добре фінансуються, а їх атаки зосереджені на корисних для їхнього уряду конкретних цілях .

Для ефективного захисту від атак професіонали з кібербезпеки повинні мати такі ж навички, як хакери, особливо хакери у чорних капелюхах. Відмінність хакера від професіонала з кібербезпеки полягає в тому, що професіонал з кібербезпеки повинен працювати у правовому полі.

Ви навіть не повинні бути працівником, щоб потрапити під дію законів про кібербезпеку. У вашому приватному житті ви можете мати можливість та вміння щоб зламати комп'ютер чи мережу іншої людини. Існує стара приказка: "Якщо можеш щось зробити, це не привід то зробити". Візьміть це до уваги. Більшість хакерів залишають сліди, незалежно від того, чи знають вони про це, і ці сліди можуть відслідковувати кіберспеціалісти.

Фахівці з кібербезпеки розвивають багато навичок, які можуть бути використані як для добра так і для зла. Ті, хто використовує свої навички у правому полі для захисту інфраструктури, мереж та конфіденційності завжди користуються великим попитом.

У більшості країн існують закони про кібербезпеку. Вони можуть мати відношення до критичної інфраструктури, мереж та конфіденційності корпоративних та приватних даних. Підприємства повинні дотримуватися цих законів.

У деяких випадках, якщо ви порушите закони про кібербезпеку під час виконання вашої роботи, то може бути покарана компанія, а ви можете втратити свою роботу. В інших випадках ви можете бути притягнуті до відповідальності, одержати штрафні санкції, а можливо і засуджені.

Загалом, якщо ви не впевнені в тому, що певна дія або поведінка є законною, то припускайте, що вона незаконна і не робіть цього. Ваша компанія може мати юридичний відділ або хтось із відділу кадрів, зможе відповісти на ваші запитання, перш ніж ви зробите щось незаконне.

Сфера законів про кібербезпеку значно новіша, ніж сама кібербезпека. Як згадувалося раніше, в більшості країн існують свої закони, і їх кількість буде збільшуватись.

Міжнародний закон про кібербезпеку є досить новим. Міжнародне багатостороннє партнерство проти кибер-загроз (*IMPACT*) - це перше, міжнародне публічно-приватне партнерство, яке зосереджується на кіберзагрозах. [*IMPACT*](http://www.impact-alliance.org/home/index.html) це глобальне партнерство світових урядів, представників промисловості та академічної спільноти, що спрямоване на покращення глобальних можливостей у боротьбі з кіберзагрозами [6].

Профілі та мотиви кібер-кіберзлочинців змінювалися з роками. Хакінг почався в 60-ті роки з телефонного фрікінгу (phone freaking або phreaking), що полягав у використанні різних звукових частот для маніпулювання телефонними системами. У середині 80-х років злочинці використовували комп'ютерні модеми для комутованих ліній для підключення комп'ютерів до мереж і застосовували програми для зламу паролів, щоб отримати доступ до даних. В наш час злочинці виходять за рамки банальної крадіжки інформації. Сьогодні злочинці можуть використовувати шкідливе ПЗ і віруси як високотехнологічну зброю. Однак, найбільша мотивація для більшості кіберзлочинців - фінансова. Кіберзлочинність стала більш прибутковою, ніж нелегальна торгівля наркотиками [6, 15, 16].

Запобігання кіберзлочинам - це складне завдання і такої універсальної речі, як «срібна куля» немає. Однак компанії, уряди і міжнародні організації почали здійснювати скоординовані дії спрямовані на те, щоб обмежити або захиститись від кіберзлочинців. Скоординовані дії включають [6, 15, 16]:

1. Створення комплексних баз даних відомих системних вразливостей і сигнатур атак (унікальна домовленість про зберігання інформації, що використовується для ідентифікації спроб зловмисників використовувати будь-яку відому вразливість). Організації по всьому світу діляться цими базами даних, щоб допомогти підготуватись та відбити велику кількість поширених атак.
2. Встановлення сенсорів раннього попередження та мереж оповіщення. Через високу вартість і неможливість моніторингу кожної мережі, організації контролюють важливі об'єкти або створюють пастки, які виглядають як важливі об'єкти. Оскільки на ці псевдоважливі цілі найчастіше здійснюються атаки, вони дозволяють попередити інших про потенційні напади.
3. Обмін інформацією в кібер-розвідці. На даний час бізнес, урядові організації і країни співпрацюють для обміну критичною інформацією про серйозні напади на найважливіші цілі, щоб запобігти подібним атакам в інших місцях. Багато країн створили агентства кібер-розвідки для міжнародної співпраці у боротьбі з великими кібератаками.
4. Спільне визначення загальних стандартів управління кібербезпекою національними і міжнародними установами. *ISO* 27000 є хорошим прикладом цих спільних зусиль.
5. Впровадження нової законодавчої бази для запобігання кібератакам і порушенням безпеки даних. Ці закони передбачають суворі покарання для кіберзлочинців, спійманих за незаконними діями.

**1.5.** **Види загроз для користувачів, їх властивості та типи кібератак**

Як було описано раніше, експерти мають бути новаторами і провидцями. Вони будують різноманітні кібер-домени в Інтернеті. Вони мають здатність розпізнавати потужність даних і використовувати її. Надалі вони створюють свої організації та надають послуги, а також захищають людей від кібератак. В ідеалі професіонали в області кібербезпеки повинні розпізнавати загрозу, яку можуть нести у собі дані, якщо вони застосовуються проти людей [6, 15].

Загрози і вразливості є основним предметом стурбованості фахівців з кібербезпеки. Головним чином вирішальними є дві ситуації:

1. Коли загроза відкриває ймовірність того, що станеться негативна подія, наприклад, відбудеться атака.
2. Коли вразливість робить ціль сприйнятливою до атаки.

Наприклад, дані в руках зловмисників можуть привести до втрати конфіденційності для власників, можуть вплинути на їх фінансове становище або поставити під загрозу їх кар'єру, чи особисті відносини. Крадіжка особистих даних - великий бізнес. Проте, *Google* і *Facebook* не обов'язково є найбільшим ризиком. Школи, лікарні, фінансові установи, державні установи, звичайні робочі місця і електронна комерція можуть становити ще більшу небезпеку.

Такі організації, як *Google* і *Facebook*, мають у своєму розпорядженні ресурси для найму дуже талановитих кіберспеціалістів для захисту своїх доменів. Оскільки все більше організацій створюють великі бази даних, що містять всі наші персональні дані, потреба в професіоналах з кібербезпеки зростає. Тому для менших підприємств та організацій залишається конкурувати за решту кіберспеціалістів. Кібер-загрози особливо небезпечні для певних галузей і даних, які вони використовують.

Візит до лікаря супроводжується додаванням інформації до електронного медичного запису (Electronic Health Record, EHR). Рецепт від сімейного лікаря стає частиною *EHR*. *EHR* містить інформацію про фізичне та психічне здоров'я та іншу персональну інформацію, яка може бути не пов'язана з медициною. Наприклад, людина зверталася за консультацією психолога в дитинстві, через серйозні зміни у сім'ї. Це буде десь відображено в її медичних документах. Крім історії хвороби і особистої інформації, EHR може також включати інформацію про сім'ю цієї людини. Існують закони, що спрямовані на захист записів у медичних картах пацієнтів.

Медичні пристрої, такі як фітнес-браслети, використовують хмарну платформу для забезпечення бездротового передавання, зберігання і відображення медичних даних. Таких як частота серцевих скорочень, кров'яний тиск і цукор у крові. Ці пристрої генерують величезну кількість медичних даних, які можуть стати частиною медичної карти пацієнта.

Дані про освіту містять інформацію про оцінки, результати тестів, відвідуваність, пройдені курси, нагороди, дипломи та дисциплінарні стягнення. Ці дані можуть містити контактну інформацію, записи про стан здоров'я і щеплення, про спеціалізовану освіту, включаючи індивідуальні освітні програми (Individualized Education Programs, IEPs).

Інформація про зайнятість може включати дані про минулу роботу та діяльність. Записи про зайнятість можуть також включати інформацію про заробітну плату і страхування. Фінансові документи можуть містити інформацію про доходи та витрати. Податкові документи можуть включати в себе виписки з кредитних карток, кредитну історію та іншу банківську інформацію.

Існує багато важливих технічних сервісів, які необхідні для роботи мережі, а в кінцевому рахунку, Інтернету. Це такі служби, як маршрутизація, адресація, іменування доменів і керування базами даних. Вани є першочерговими цілями для кіберзлочинців.

Злочинці використовують інструменти перегляду пакетів (packet-sniffing) для захоплення потоків даних, що проходять через мережу. Це означає, що всі конфіденційні дані, такі як імена користувачів, паролі та номери кредитних карт, піддаються ризику. Інструменти перегляду пакетів моніторять і записують всю інформацію, що проходить через мережу. Злочинці можуть також використовувати підставні пристрої, такі як відкриті точки доступу Wi-Fi. Якщо злочинець встановлює їх близько до громадського місця, наприклад, кафе, люди, нічого не підозрюючи, можуть увійти в систему, а інструмент перегляду пакетів (сніфер пакетів) скопіює їх особисту інформацію.

Служба доменних імен (*Domain Name Service, DNS*) транслює доменне ім'я, наприклад *www.facebook.com*, в його числову *IP*-адресу. Якщо *DNS*-сервер не знає *IP*-адресу, він надішле запит на інший *DNS*-сервер. При підміні *DNS* (*DNS* *spoofing*), або це ще називають отруєнням *DNS* кешу (*DNS* cache poisoning), злочинець вводить недостовірні дані в кеш-пам'ять *DNS*-транслятора. Атаки отруєння кешу *DNS* використовують вразливість у програмному забезпеченні протоколу *DNS*, яка змушує *DNS*-сервери перенаправляти трафік для певного домену на комп'ютер злочинця, а не до законного власника цього домену.

Пакети переносять дані через мережу або Інтернет. Підробка пакетів (*packet* *forgery*) або як ще називають ін'єкція пакетів (*packet* *injection*), заважає встановленому мережному зв'язку, створюючи пакети таким чином, ніби вони є частиною цього сеансу зв'язку. Ця підробка дозволяє злочинцеві пошкодити або перехопити пакети. Цей процес дозволяє злочинцеві захопити авторизоване з'єднання або позбавити користувачів можливості використовувати певні мережні служби. Професіонали називають це атакою «людина по середині» (*man*-*in-the*-*middle*).

Ключовими галузями промисловості є мережні інфраструктурні системи, такі як виробництво, енергетика, зв'язок та транспорт. Наприклад, розумна мережа електропостачання (*smart* *grid*) - це удосконалена система генерації та розподілу електроенергії. Мережа електропостачання передає електроенергію від центральних генераторів до великої кількості клієнтів. Розумна мережа використовує інформацію для створення сучасної автоматизованої системи постачання електроенергії. Світові лідери визнають, що захист цієї інфраструктури є критичним для захисту економіки.

За останнє десятиліття кібератаки, подібні Stuxnet, довели, що кібератаки можуть успішно знищити або перервати роботу критичних інфраструктур. Зокрема, атака Stuxnet була націлена на систему контролю і збору даних (*Supervisory* *Control* *and* *Data* *Acquisition*, *SCADA*), яка використовувалась для контролю і моніторингу промислових процесів. *SCADA* може бути частиною різних технічних процесів у промисловості, виробничих, енергетичних і комунікаційних системах. Натисніть [тут](https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en" \o "https://www.ted.com/talks/ralph_langner_cracking_stuxnet_a_21st_century_cyberweapon?language=en) , щоб переглянути додаткову інформацію про атаку *Stuxnet*.

Кібератака може привести до знищення або зупинки таких галузей, як телекомунікації, транспорт, виробництво електроенергії та системи її розподілу. Це може також порушити роботу сектору фінансових послуг. Однією з проблем в середовищах, де використовується *SCADA*, є той факт, що розробники не підключали *SCADA* до традиційного *ІТ*-середовища та Інтернету. Тому вони не врахували питання кібербезпеки на етапі розробки цих систем. Як і в інших галузях, організації, що використовують системи *SCADA*, визнають цінність збору даних для покращення виробництва і зниження витрат. Загальна тенденція полягає в тому, щоб підключити *SCADA*-системи до традиційних *ІТ*-систем. Однак це підвищує вразливість підприємств, що використовують системи *SCADA*.

Вразливості програмних продуктів на сьогоднішній день базуються на помилках програмування, вразливостях протоколів або некоректної конфігурації системи. Кібер-злочинцю залишається просто використати одну з них. Наприклад, звичайна атака включає в себе створення певного потоку даних на вхід в програму для змін у програмі, які приводять до її збою. Такі збої створюють портал для несанкціонованого входу в програму або можуть викликати витік інформації.

На сьогоднішній день зростає витонченість кібератак. Постійна загроза підвищеної складності (Advanced Persistent Threat) - це безперервна довготермінова комп'ютерна атака, яка спрямовується проти конкретного об'єкта. Злочинці зазвичай роблять вибір цілей для APT з бізнес або політичних мотивів. APT відбувається тривалий період часу з високим ступенем секретності та з використанням складного шкідливого ПЗ.

Алгоритмічні атаки можуть відстежувати дані, що автоматично повідомляються системою, наприклад дані про споживану комп'ютером електроенергію. Та можуть використовувати цю інформацію для вибору цілей атаки або помилкової активації аварійних сповіщень. Алгоритмічні атаки також можуть призвести до відмови комп'ютера, змушуючи його надмірно використовувати пам'ять або перевантажуючи центральний процесор. Алгоритмічні атаки є більш витонченими, тому що вони використовують компоненти ОС, які застосовуються для енергозбереження, зниження відмов системи та підвищення її ефективності.

Нарешті, нове покоління атак передбачає розумний вибір жертв. У минулому для нападу вибирали слабозахищені або найбільш вразливі жертви. Однак, через підвищення уваги до виявлення та ізоляції кібератак, кіберзлочинці повинні бути більш обережними. Вони не можуть ризикувати через раннє виявлення, бо фахівці з кібербезпеки "закриють ворота" вразливості. В результаті, більш складні атаки будуть запускатися тільки в тому випадку, якщо атакуючий зможе підібрати характерний цільовий об'єкт.

Інтегроване (федеративне) керування ідентифікацією застосовують у компаніях, які дозволяють своїм користувачам використовувати одні і ті ж ідентифікаційні дані, для отримання доступу до мереж усіх підприємств групи. Це розширює масштаб і збільшує ймовірність каскадного ефекту під час атаки.

Інтегроване керування ідентифікацією поєднує електронну ідентичність суб'єкта через окремі системи керування ідентифікацією. Наприклад, суб'єкт може увійти на *Yahoo*! з обліковими даними *Google* або *Facebook*. Це приклад входу в систему через дані соціальних мереж.

Метою інтегрованого керування ідентифікацією є автоматична передача ідентифікаційної інформації у межах захищеної групи. З точки зору окремого користувача це означає єдиний ідентифікаційний вхід в Інтернет.

Дуже важливо, щоб організації ретельно перевіряли ідентифікаційну інформацію, яка надається партнерам. Номери соціального страхування, імена та адреси можуть дозволяти зловмисникам, що викрадають персональну інформацію, викрасти її у партнера для здійснення шахрайства. Найбільш поширений спосіб захисту інтегрованого керування ідентифікацією - зв'язати логін з авторизованим пристроєм.

Зловмисне програмне забезпечення або шкідливе ПЗ - це термін, який використовується для опису програмного забезпечення, призначеного для порушення роботи комп'ютера або отримання доступу до комп'ютерних систем без відому або дозволу користувача. Зловмисне програмне забезпечення стало загальним терміном, який використовується для опису всіх ворожих або нав'язливих програм. Термін "зловмисна програма" описує комп'ютерні віруси, черв'яки, троянські коні, програми-вимагачі, шпигунські програми, рекламне програмне забезпечення, псевдоантивіруси та ін. Деяке шкідливе ПЗ виявити легко, дію інших виявити практично неможливо.

Кіберзлочинці досягають кінцевих пристроїв користувача, встановлюючи на них зловмисне програмне забезпечення. Натисніть кнопку «Перегляд», щоб переглянути анімацію для трьох найбільш поширених типів зловмисного програмного забезпечення.

Вірус – це шкідливий програмний код, прикріплений до виконуваного файлу, наприклад, легітимної програми. Для більшості вірусів необхідно, щоб користувач запустив заражену програму, також вони можуть активуватися в конкретний час або дату. Комп'ютерні віруси зазвичай поширюються одним із трьох способів: через знімні носії; завантажуються з Інтернету; через вкладення електронної пошти. Віруси можуть бути нешкідливими і просто виводити рисунок на екран, або можуть бути руйнівними, як наприклад ті, що змінюють або видаляють дані. Щоб уникнути виявлення, вірус мутує. Комп'ютер може бути заражений вірусом просто в результаті того, що користувач відкрив файл. Деякі віруси вражають завантажувальний сектор або файлову систему флеш-накопичувачів USB, а з них можуть поширюватися на системний жорсткий диск комп’ютера. Також зараження вірусами може відбуватися при виконанні конкретної програми. Після активації вірусу він постійно заражатиме інші програми на комп'ютері або на інших комп'ютерах в мережі. Вірус Меліса став прикладом вірусу, який поширювався електронною поштою. Меліса завдала шкоди десяткам тисяч користувачів і, за приблизними оцінками, спричинила збитків на 1.2 мільярда доларів. Натисніть [тут](http://www.whoishostingthis.com/blog/2015/06/01/8-worst-viruses/) щоб дізнатись більше про віруси.

Черв'яки – це зловмисний код,, який поширюється самостійно, використовуючи вразливості мережної інфраструктури. Зазвичай черв'яки уповільнюють роботу мережі. На відміну від вірусів, які потребують запуску зараженої програми-носія, черв'яки можуть працювати самостійно. Після первинного інфікування черв'яки більше не потребують участі користувача. Після зараження вузла черв'як має змогу розповсюджуватися у компютенерній мережі із значною швидкістю. Черв'яки діють за єдиним принципом. Всі вони використовують певну слабкість системи, мають механізм мастабування і виконують певну зловмисну дію.

Черв'яки відповідальні за деякі найбільш руйнівні кібератаки у мережі. Наприклад, в 2001 році черв'як *Code* *Red* заразив 658 серверів. У подальшому, протягом 19 годин цей черв'як заразив більше ніж 300 тисяч серверів.

Шкідливе програмне забезпечення, що наносить шкоду маскуючись під дії користувача системи, наприклад онлайн-гри, має назву Троянський кінь. Фактично воно використовує профіль користутвача та його дії. Відміності від вірусу поролягає у тому, що він прив'язується до статичних файлів, таких як файли зображень, аудіофайли або ігри.

Програми-вимагачі блокують комп'ютерну систему, або дані, які вона містить, доки жертва не сплатить викуп. Програми-вимагачі кодують цифрові дані на машині за допомогою коду, що невідомий користувачу. Користувач має сплатити викуп зловмисникам, щоб зняти обмеження.

Часто такі програми використовують слабкі місця конкретної машини для її зупинки. Програми-вимагачі розповсюджуються аналогічно до Троянського коня через завантаження файлів або вразливості програмного забезпечення.

Оплата, яку має внести жертва, зазвичай відбувається через платіжну систему, яка не дозволяє відслідковувати отримувача. Після того, як жертва сплатить викуп, зловмисники надають їй програму, що розшифровує файли або надсилають код для розблокування. Натисніть [тут](http://www.exterminate-it.com/malpedia/ransomware-category) щоб дізнатись більше про програми-вимагачі.

Термін *backdoor* відноситься до програми або коду, доданого зловмисником, який скомпроментував систему. *Backdoor* обходить стандартну аутентифікацію, яка використовується для доступу до системи. До найбільш поширених програм цього типу відносяться *Netbus* і *Back* *Orifice*, що надають віддалений доступ до системи неавторизованим користувачам. Мета backdoor - надавати кібер-злочинцям доступ до системи в майбутньому, навіть після того, як організація виправить вразливість, яка була використана для атаки на систему. Зазвичай, щоб встановити *backdoor*, злочинці використовують авторизованих користувачів, які несвідомо запускають троянську програму на своєму ПК.

Руткіт модифікує операційну систему для створення чорного ходу. Потім зловмисники використовують для віддаленого доступу до комп'ютера. Більшість руткітів використовують *backdoor* вразливості програмного забезпечення для підвищення рівня привілеїв (ескалації прав доступу) та модифікації системних файлів. Ескалація привілеїв можлива через помилки програмування або недоліки проектування і дозволяє зловмисникам отримати підвищений рівень доступу до мережних ресурсів та даних. Також руткіти здійснюють зміни в системи перевірки стану та інструментах моніторингу, що дуже ускладнює виявлення зловмисного ПЗ такого типу. Часто для знищення руткіту доводиться перевстановити операційну систему.

Кілька простих кроків допоможуть захистити ваш комп'ютер від усіх видів зловмисного програмного забезпечення [6, 17].

1. Антивірусна програма - Більшість антивірусних пакетів успішно виявляють найпоширеніші форми шкідливого ПЗ. Проте щоденно кіберзлочинці розробляють і розповсюджують нові загрози. Тому ключем до ефективного захисту проти вірусів є постійне оновлення бази вірусних сигнатур. Сигнатура для віруса - це як відбиток пальця для людини. Вона ідентифікує характерні елементи зловмисного коду, за якими його можна розпізнати.
2. Актуальне ПЗ - багато форм зловмисного ПЗ досягають своїх цілей через використання вразливостей програмного забезпечення як в операційних системах, так і в застосунках. Раніше вразливості операційної системи були основним джерелом проблем, на сьогоднішній день найбільший ризик становлять вразливості застосунків. В той час, як розробники операційних систем все швидше реагують на нові загрози, більшість розробників прикладного ПЗ на жаль нехтують цим.

Електронна пошта – це універсальний сервіс, що використовується мільярдами людей у всьому світі. Як один з найбільш популярних сервісів, електронна пошта стала головною вразливістю для користувачів та організацій. Спам, також відомий як небажана пошта, або небажаний електронний лист. У більшості випадків спам - це один зі способів реклами. Однак спам може містити небезпечні посилання, зловмисне ПЗ або оманливий вміст. Кінцевою метою такого спаму є отримання конфіденційної інформації користувача, такої як номер соціального страхування або інформація про банківський рахунок. Більшість спаму надходить з великої кількості комп'ютерів, які розташовані в мережах, заражених вірусом або Інтернет-черв'яком. Ці скомпрометовані комп'ютери надсилають максимально можливу кількість повідомлень електронної пошти.

Навіть за умови реалізації функцій захисту від спаму, повністю виключити небажану пошту все ж не вдасться. Ознайомтеся з деякими найбільш поширеними характеристиками спаму:

1. В електронному листі відсутня тема.
2. Електронний лист вимагає оновлення облікового запису.
3. Текст електронного листа містить слова з помилками або дивну пунктуацію.
4. Посилання в електронному листі є довгими та/або незрозумілими.
5. Електронний лист виглядає як листування з реально існуючою організацією.
6. Електронний лист вимагає від користувача відкрити вкладення.

Якщо користувач отримує електронний лист, що відповідає одному або декільком з цих характеристик, йому не варто відкривати цей лист або будь-які вкладення. Зазвичай політика використання електронної пошти організації вимагає, щоб користувач, який отримав електронний лист такого типу, повідомив про це співробітникам відділу кібербезпеки. Майже всі поштові сервіси фільтрують спам. На жаль, спам все одно створює навантаження на мережу і сервер отримувача.

Шпигунське ПЗ – це програмне забезпечення, яке дозволяє злочинцям отримувати інформацію про дії користувача за комп'ютером. Шпигунські програми часто містять засоби відстеження активності, набраних на клавіатурі символів та перехоплення даних. Для того, щоб обійти заходи безпеки, шпигунські програми часто змінюють налаштування безпеки. Шпигунські програми часто прив'язуються до легального ПЗ або розповсюджуються троянами. Багато веб-сайтів, які поширюють умовно-безкоштовні програми містять шпигунські програми.

Рекламне ПЗ зазвичай відображає надокучливі спливаючі вікна з метою отримання доходу їх авторами від реклами. Зловмисне програмне забезпечення може аналізувати інтереси користувача, відстежуючи які веб-сайти він відвідує. Потім зловмисне ПЗ може надсилати спливаючу рекламу, яка відповідає тематиці цих сайтів. Деякі версії програмного забезпечення автоматично встановлюють рекламне ПЗ. Деяке рекламне ПЗ дійсно забезпечує тільки доставку реклами, але часто рекламне ПЗ поширюється разом зі шпигунським.

Наступним розглянемо осбливу різновидність кіберзлочиності фішинг. Злодії у кіберпросторі, маскуються під фізичну чи юридичну особу, за допомогою електроної пошти, систем миттєвого обміну повідомленнями або соціальних мережі збирають інформацію про реєстраційні дані або дані облікового запису. Фішинг відбувається, коли зловмисник надсилає шахрайського електронного листа, який виглядає як такий, що цілком безпечний. Метою є спонукання абонента до встановлення шкідливого програмного забезпечення на свою машину або розголошення своїх персональних даних. У якості приклада можливо навести одержання сфальшованого листа від якоїсь організації з прозицією перейти за посиланням для одержання бонусів, грошей або призу. Після переходу на шахрайську сторінку у користуача, як правило, запитуються особисті дані або встановлюється шкідливе програмне забезпечення.

Спрямований фішинг – це випадок коли листи цілеспрямована надсилаються обраній особі. Для досягнення мети зловмисники попередньо вивчають жертву. Встановлюють чим вона цікавиться, які має потреби та проблеми. Потім це все виекористовується під час фальшування листів.

Голосовий фішинг – це фішинг за допомогою технологій голосових комунікацій. Злочинці можуть робити фальшиві дзвінки, представляючись довіреними організаціями, за допомогою технології передачі голосу через *IP* (*VoIP*). Жертви також можуть отримати записане повідомлення, яке виглядає легітимним. Таким чином злочинці намагаються отримати номери кредитних карток або іншу інформацію, щоб викрасти персональні дані жертви. Успішність голосового фішингу пояснюється довірою людей до телефонної мережі.

Атака типу "Відмова в обслуговуванні" (*DoS*) - є різновидом мережної атаки. Результатом *DoS*-атаки є переривання доступу користувачів, пристроїв або застосунків до мережних сервісів. Існує два основних типи *DoS*-атак:

1. Перевантаження великою кількістю трафіку - Нападник надсилає величезну кількість даних з такою швидкістю, що мережа, хост або застосунок не встигає їх обробляти. Це спричиняє уповільнення передачі або реагування, іноді призводить до аварійного завершення роботи пристрою чи сервісу.
2. Пакети неправильного формату (Maliciously Formatted Packets) - Нападник надсилає пакет даних неправильного формату хосту або застосунку і одержувач не може його обробити. Наприклад, програма не може ідентифікувати пакети, що містять помилки або неналежним чином відформатовані. Це призводить до того, що приймаючий пристрій буде працювати дуже повільно або припинить роботу взагалі.

*DoS* – атаки становлять серйозний ризик, оскільки вони можуть легко переривати обмін інформацією та заподіяти значну втрату часу й грошей. Ці атаки відносно прості для виконання навіть некваліфікованим нападником.

Метою атаки «відмова в обслуговуванні» є припинення доступу для авторизованих користувачів через недоступність мережної інфраструктури (згадайте три основні принципи безпеки: конфіденційність, цілісність та доступність).

Розподілена *DoS* атака (*DDoS*) подібна до атаки *DoS*, але вона походить з декількох скоординованих джерел. Наприклад, атака *DDoS* може розвиватися наступним чином [6, 15]:

Зловмисник створює мережу заражених хостів, яка називається ботнетом і складається з комп'ютерів-зомбі. Зомбі - це заражені хости. Для контролю над зомбі зловмисник використовує спеціальну керуючу систему. Комп'ютери-зомбі постійно сканують мережу і заражають інші хости, створюючи ще більше нових зомбі. Після такої підготовки хакер через керуючу систему дає наказ ботнету розпочати *DDoS* атаку.

*Sniffing* є дуже схожим на підглядання за людиною в реальному світі. Хакери досліджують весь мережний трафік, який проходить через їх мережну інтерфейсну карту (*NIC*), незалежно від того, кому він адресований. Злочинці виконують аналіз трафіку в мережі за допомогою програмного забезпечення, апаратного пристрою або їх комбінації. Як показано на рисунку, *Sniffing* переглядає весь мережний трафік або виконується фільтрація за певним протоколом, сервісом чи навіть за рядком символів, таких як ідентифікатор користувача або пароль. Деякі мережні аналізатори можуть перевіряти весь трафік і навіть змінювати його частково або повністю.

Підміна – це атака шляхом імперсоніфікації, яка відбувається за рахунок використання довірчих відносин між двома системами. Якщо дві системи підтримують єдину аутентифікацію, користувач, який увійшов до однієї системи, може не проходити повторно процес аутентифікації для доступу до іншої системи. Зловмисник може скористатися цими довірчими відносинами, відправивши пакет до однієї системи, який виглядає як такий, що надійшов з іншої довіреної системи.

Існує кілька типів атак з використанням підміни.

1. Підміна *MAC*-адреси відбувається, коли один комп'ютер приймає пакети даних, адресовані на *MAC*-адресу іншого комп'ютера.
2. IP-spoofing надсилає *IP*-пакети з підробленої *ІР*-адреси джерела, щоб замаскувати свою справжню адресу.
3. Протокол визначення адрес (*ARP*) - це протокол, який перетворює *IP*-адреси в *MAC*-адреси для передачі даних. При *ARP* підміні зловмисник розсилає підроблені *ARP* повідомлення локальною мережею для того, щоб зв'язати свою *MAC*-адресу з *IP*-адресою авторизованого користувача мережі.
4. Система доменних імен (*DNS*) асоціює доменні імена з *IP*-адресами. При підміні *DNS* відбувається модифікація *DNS*-сервера для перенаправлення певного доменного імені на іншу адресу, контрольовану злочинцем.

Злочинець, який виконує атаку Man-in-the-middle (*MitM*), перехоплює повідомлення, якими обмінюються комп'ютери, щоб викрасти інформацію, яка проходить мережею. Злочинець також може маніпулювати повідомленнями та передавати підставні дані між хостами, оскільки вузли не усвідомлюють, що відбулася модифікація повідомлень. *MitM* дозволяє злочинцю контролювати пристрій без відому користувача.

*Man-In-The-Mobile* (*MitMo*) (людина-в-мобільному) – різновид атаки "*Man-in-the-middle* . При *MitMo* зловмисник отримує контроль над мобільним пристроєм. Заражений мобільний пристрій пересилає конфіденційну інформацію користувача нападникам. *ZeuS* є прикладом експлойта з можливостями *MitMo*, який дозволяє атакуючим непомітно перехоплювати *SMS*-повідомлення 2-етапної авторизації, які надходять користувачам. Наприклад, коли користувач створює обліковий запис *Apple*, він повинен надати телефонний номер для отримання *SMS* з тимчасовим кодом підтвердження. Зловмисне ПЗ відстежує ці повідомлення та передає інформацію злочинцям.

При реалізації атаки з повтором зловмисник перехоплює частину даних, які пересилаються між двома хостами, а потім повторно передає записане повідомлення. Такий спосіб дозволяє обійти механізми аутентифікації.

Атака нульового дня (*zero-day attack*), яку іноді називають загрозою нульового дня (*zero-day threat*), – це комп'ютерна атака, яка намагається використати вразливості ПЗ, що досі невідомі постачальнику програмного забезпечення або які він приховує. Термін нульова година (*zero hour*) описує момент, коли хтось виявляє експлойт (шкідливий програмний код). Впродовж часу, доки виробник програмного забезпечення розробляє та випускає виправлення, мережа залишається вразливою для цього експлойту. Для захисту від цих стрімких атак професіоналам з мережної безпеки необхідно більш ретельно продумати архітектуру мережі. В наш час стримувати декілька вторгнень до системи одночасно у різних точках майже не можливо.

Клавіатурний шпигун – це програма, яка записує або вносить в спеціальний журнал натискання клавіш користувачем системи. Злочинці можуть реалізовувати кейлогери за допомогою ПЗ, встановленого на комп'ютері або через обладнання, фізично приєднане до комп'ютера. Зловмисник налаштовує ПЗ клавіатурного шпигуна таким чином, щоб воно відправляло зібрану в журналі інформацію електронною поштою. Перехоплені та записані до лог-файлу натискання клавіш можуть розкрити імена користувачів, паролі, відвідані веб-сайти та іншу конфіденційну інформацію.

Клавіатурні шпигуни можуть бути легальними, комерційними програмами. Батьки часто купують таке програмне забезпечення для відстеження поведінки дітей в Інтернеті та з'ясування того, які веб-сайти вони відвідують. Більшість анти-шпигунських програм здатні виявити та видалити несанкціоновані кейлогери. Хоча кейлогери не є незаконними програмами, але злочинці використовують їх для досягнення своїх незаконних цілей.

Організація може запровадити низку заходів для захисту від різноманітних атак. Налаштуйте міжмережні екрани так, щоб відхиляти будь-які пакети, що надходять ззовні мережі, але мають адреси, які вказують на їх походження з внутрішньої мережі. Така ситуація є незвичайною, і це вказує на те, що кібер-злочинець спробував здійснити атаку з підміною адреси [21].

Щоб запобігти *DoS* та *DDoS* атакам, переконайтеся, що патчі та оновлення є актуальними, розподіляйте навантаження між серверними системами та блокуйте зовнішні *ICMP* пакети на межі периметру. Мережні пристрої використовують *ICMP*-пакети для надсилання повідомлень про помилки. Наприклад, команда ping використовує *ICMP* пакети для перевірки чи може пристрій взаємодіяти з іншими пристроями в мережній інфраструктурі.

Системи можуть попередити повторні напади, шифруючи трафік, використовуючи криптографічну аутентифікацію та включаючи часові мітки до кожної частини повідомлення.

## **Висновки до першого розділу**

У першому розділі кваліфікаційгної роботи бакалавра автором було проведено аналіз існуючих загроз безпеки в інфокомунікаційних мережах сучасності. Визначено, що із зростанням рівня впровадження інформаційних технологій у життя особистості, суспільства і держави, зростає рівень небезпеки у кібернетичному просторі. На адекватне реагування викликам сучасності потреббує нарощення система заходів щодо протидії викликам у кіберпросторі.

Автором розглянуто стан інформаційної безпеки в Україні в умовах ведення гібрідної війни РФ проти України. Зроблено висноки про різке збільшення кібератак з боку РФ.

Розглянуті загальні тенденції у забезпеченні кібербезпеки на всіх рівнях. Систематизовані типи загроз для користувачів. Розглянуті їх властивості.

**РОЗДІЛ** **2  
МЕТОДИ АВТОМАТИЗОВАНОГО НАЛАШТУВАННЯ КОНФІГУРАЦІЙ БЕЗПЕКИ МЕРЕЖЕВОГО ОБЛАДНАННЯ**

**2.1. Сучасні методи оркестрації та управління конфігурацією**

Для збільшення швидкості налаштування безпеки мережі, відновлення її функціонування та коректної роботи в разі пошкоджень та збоїв актуальною буде використання оркестрації.

Оркестрацію найкраще описати на прикладі. Припустимо, у вас є додаток з високим трафіком і вимогами високої доступності. Через ці вимоги звичайно потрібно розгорнути як мінімум на 3+ комп'ютерах, тому в разі збою хоста ваш додаток буде як і раніше принаймні для двох інших. Очевидно, це всього лише приклад, і ваш сценарій використання, ймовірно, буде мати свої власні вимоги, але ви зрозуміли ідею [18-20].

Розгортання додатку без використання оркестрації зазвичай займає багато часу і схильне до помилок, оскільки вам доведеться вручну підключати *SSH* до кожного комп'ютера, запускати додаток і потім постійно стежити за тим, щоб воно працювало так, як ви очікуєте.

Але за допомогою інструментів оркестрації ви, як правило, можете розвантажити більшу частину цієї ручної роботи і дозволити автоматизації виконувати важку роботу. Одна з чудових можливостей оркестрації полягає в тому, що ви можете розгорнути додаток на декількох хостах за допомогою однієї команди. Крім того, якщо один з підтримуваних вузлів виходить з ладу у вашій мережі, інші вузли автоматично отримають навантаження, і ваш додаток продовжить працювати як зазвичай.

Нині існує велика кількість програм, що можуть налаштовувати, швидко відновлювати і управляти конфігурацією. Широко використовуваними є *Ansible*, *Puppet*, *CHEF*, *SaltStack* та *Terraform*.

***Ansible***

Це спеціалізована програма. Вона призначена для здійснення управління конфігурацією, оркестровки, встановлення додатків, розпаралелювання відпрацювання групою машин типових завдань. Первиний код *Ansible* реалізований на програмній мові *Python.* Для одержання програми потребується ліцензія *GPLv3*.

*Ansible* має ряд безаперечних переваг. Це проста і сприятлива для користувача мова управління конфігурацією, реалізації розпаралелювання виконання завдань, не потрібність встановлення на винесені машини спеціалізовани програм-агентів, реалізація спроможності функціонування без прав root. Програма *Ansible* не така складна, як спеціалізовані програми *CFEngine*, *Puppet* і *Chef*. Проте, має виликий спектр спроможностей при одночасній гнучкісті управління.

Вагома перевага використання *Ansible* у відсутності необхідності здійснювати інсталяцію клієнта на цільових системах. Для користування *Ansible* потрібно створити «плейбуки» у форматі *YAML* у якому прописати необхідні системи, що управляються. Що таке «Плейбук»? Це опис фактичного стану ресурсів системи у кожний кокретний відрізок часу її функціонування. При цьому до опису входять пакети програм, що встановлені, функціонуючі служби, створені у системі файли та інші характеристики стану системи. Програма *Ansible* слідкує за знаходженням кожного із ресурсів системи у необхідному стані та вживає заходів до їх повернення до необхідного стану у разі необхідності.

Система інтегрованих функціональних модулів призначена для реалізації завдань. Завданя реалізовується через його назву, модуль з встановленими параметрами, що використовується для виконання завдання.

Категорії модулів Ansible і виконувані ними завдання:

* *Cloud*: підтримка *Amazon* *EC2* / *ECS* / *S3*, *Azure*, *Cloudstack*, *Digital* *Ocean*, *Docker*, *LXC*, *OpenStack*, *Rackspace*, *VMware* і ін;
* *Clustering*: підтримка *Consul*, *ZooKeeper* (англ.), *Kubernetes*;
* *Command*: виконують консольні команди і скрипти;
* *Database*: підтримка баз даних *MySQL*, *PostgreSQL*, *Vertica*, *MongoDB*, *Redis*, *Riak*;
* *File*: робота з файлами - копіювання, синхронізація, модифікація, перевірка, архівування і т.д.;
* *Inventory*: робота з іменами хостів або їх ip-адресами;
* *Messaging*: підтримка *RabbitMQ*;
* *Monitoring*: підтримка систем моніторингу *DataDog*, *Nagios*, i тощо;
* *Network*: робота з мережевим обладнанням і ПО *F5* *BIG*-*IP*, *Cisco* *IOS* / *NXOS*, *Juniper* *JunOS*, *OpenSwitch*, *Cumulus* *Linux*;
* *Notification*: відсилаються повідомлення в *Campfire*, *HipChat*, *Jabber*, *Pushbullet*, *Slack*, через *email* / *sms*;
* *Packaging*: робота з програмами керування пакунками *apt*, *FreeBSD* *Ports*, *Gentoo*, *homebrew*, *pacman*, *opkg*, *Red Hat software channels, yum, xbps, zypper*;
* *Source* *Control*: робота з системами контролю версій *git*, *mercurial*, *subversion*;
* *System*: робота з компонентами *Linux* / *Unix* систем - *cron*, *iptables*, *LVM*, *SELinux*, *sshd*, *zfs*;
* *Utilities*: реалізують внутрішню логіку плейбук;
* *Web* *Infrastructure*: робота з *Apache*, Dijango, *JiBoss*, *JIRA*;
* *Windows*: робота з компонентами *Windows*, в тому числі *IIS*, *Windows* *Firewall*, реєстром.

Наступним розглянемо *Puppet.* Він призначений для централізованого управління конфігурацією операційних систем і програмного забезпечення, встановлено на декількох машинах. По суті, Puppet багатоплатформовий клієнт-серверний додаток. Він реалізований мовою компютерного програмування *Ruby*.

*Puppet* значно спрощує налаштувати і управління всіма мережами на основі операційних систем *Red Hat CentOS, Fedora, Debian, Ubuntu, OpenSUSE, Solaris, BSD, Mac OS X і Microsoft Windows* (через *cygwin*).

Програма *Puppet* значно поширена серед світової IT спільноти. Вона використовується *Google*, *Fedora* *Project*, Стенфордський університет, *Red* *Hat*, *Siemens* *IT* *Solution*, *Badoo* і *SugarCRM*.

***Chef***

*Chef* - система управління конфігураціями, написана на *Ruby* (клієнтська частина) і *Erlang* (серверна частина). Для опису конфігурацій застосовувалася предметно-орієнтована мова. Система призначена для спрощення завдань налаштування і підтримки безлічі серверів і може інтегруватися в хмарні платформи, такі як *Rackspace* і *Amazon* *EC2*, для автоматизації управління поточними процесами настройки нових серверів.

Користувач *Chef* створює певні «рецепти» з описом того, як управляти серверними додатками (наприклад, *Apache*, *MySQL* або *Hadoop*) і їх налаштувань.

Під виразом «Рецепт» розуміється опис необхідного стану ресурсів системи в конкретний момент часу. До такого стану відносяться встановлені пакети програм, запущені служби, створені файли. Завданням *Chef* є перевірка правільності налаштування ресурсів системи і внесення правок до їх стану за умови, що вони не відповідають очікуваному.

*Chef* має спороможність функціонувати у режимах клієнт-сервер і автономної конфігурації (*chef*-*solo*). У режимі клієнт-сервер клієнт посилає на сервер різні властивості хоста, на якому він розташований. На стороні сервера використовується *Solr* для індексування властивостей і надання *API* для запиту інформації клієнтом. «Рецепти» можуть запитувати ці властивості і використовувати отримані дані для настройки хоста.

Зазвичай використовується для управління *Linux*-вузлами, але останні версії підтримують *Windows* .

Поряд з *CFEngine*, *Bcfg2* і *Puppet* вважається однією з найбільш популярних систем управління конфігураціями для *Linux*. Іншими прикладами є *Ansible*, *SaltStack*, а також Desiired *State* *Configuration* для i.

Програма *SaltStack* - це система управління конфігураціями і віддаленого виконання операцій. Є програмним забезпеченням з відкритим вихідним кодом, написаним на *Python*. Воно започатковано у 2011 році Томасом Хатч (Thomas Hatch). Підтримує підхід *IaaS* для розгортання та управління хмарними обчисленнями.

Двома головними складовими *SaltStack* є *Salt* *Master* ( «майстер») і *Salt* *Minion* ( «ставленик», «наближений», «міньйон»). Майстер є головною службою до якої підключаються «ставленики» для отримання конфігурації. Існують дві головні функції *SaltStack*. Це віддалене виконання операцій (remote execution) і управління конфігураціями. Віддалене виконання функцій *Python* є основою для реалізації масштабованої та управляємої конфігурації машин, з встановленими на них «ставлениками» .

Майстер і «ставленики» взаємодіють за допомогою проміжного програмного забезпечення. Воно орієнтоване на обробку повідомлень. Майстер запускає повідомлення в чергу з якої їх отримують «ставленики». Для зворотного зв'язку використовується інша чергу. Спочатку для обміну повідомленнями використовувався *ZeroMQ*, але кластери обслуговуються серверів часом мають більш десяти тисяч машин, тому на зміну *ZeroMQ* був задуманий заснований на *UDP* *RAET* (англ. Reliable Asynchronous Event Transport - «надійний асинхронний протокол для транспорту подій»).

У 2014 році до складу *Salt* був включений *Salt* Cloud, який додає в *SaltStack* рівень абстракції для роботи з різними постачальниками хмарних платформ.

**2.2. Порівняння *Ansible*, *Chef*, *Puppet* та *SaltStack***

Поширення віртуалізації в поєднанні зі зростаючою міццю стандартних серверів і доступністю хмарних обчислень привело до значного збільшення числа серверів, якими необхідно управляти як всередині організації, так і без неї. Там, де ми колись обходилися стійками з фізичними серверами, до яких ми могли звертатися в центрах обробки даних, ми тепер повинні управляти набагато більшою кількістю серверів, які можуть бути розподілені по всьому світу.

Тут вступають в гру інструменти управління центрами обробки даних і управління ними. У багатьох випадках ми управляємо групами ідентичних серверів, запускаючи ідентичні програми та сервіси. Вони розгорнуті на платформах віртуалізації в організації або працюють як хмарні або розміщені примірники у віддалених центрах обробки даних. У деяких випадках ми можемо говорити про великих установках, які існують тільки для підтримки дуже великих додатків або великих установок, які підтримують безліч невеликих сервісів. У будь-якому разі не можна скидати з рахунків можливість змахнути паличкою і змусити їх усіх підкоритися волі адміністратора. Це єдиний спосіб керувати цими великими і зростаючими інфраструктурами.

*Puppet*, *Chef*, *Ansible* і *Salt* були створені з тією ж метою: спростити настройку та обслуговування десятків, сотень або навіть тисяч серверів. Це не означає, що дрібні магазини не отримають вигоду від цих інструментів, оскільки автоматизація і оркестровка зазвичай полегшують життя в інфраструктурі будь-якого розміру.

Детально розглянувши кожен з цих чотирьох інструментів, вивчивши їх дизайн і функції і було визначено, що, хоча деякі з них мають більш високий бал, ніж інші, є місце для кожного з них, в залежності від цілей розгортання. Тут я підсумовують мої висновки.

*Puppet*, можливо, володіє найбільшою часткою розуму з чотирьох. Це найбільш повний з точки зору доступних дій, модулів і призначених для користувача інтерфейсів. *Puppet* є загальну картину оркестровки центрів обробки даних, що охоплює практично кожну операційну систему і пропонує глибокі інструменти для основних операційних систем. Початкове налаштування відносно проста, вимагає установки головного сервера і клієнтських агентів в кожній системі, якої потрібно управляти.

Звідти *CLI* (інтерфейс командного рядка) є простим, що дозволяє завантажувати і встановлювати модуль за допомогою команди puppet. Потім необхідно внести зміни в файли конфігурації, щоб адаптувати модуль для необхідного завдання, і клієнти, які повинні отримати інструкції, будуть робити це при реєстрації на головному сервері або за допомогою примусової відправки, яка відразу ж ініціює зміни.

Існують також модулі, які можуть надавати і налаштовувати екземпляри хмарного сервера і екземпляри віртуального сервера. Всі модулі та конфігурації побудовані на специфічному для *Puppet* мовою на основі *Ruby* або самого *Ruby* і, таким чином, зажадають досвіду програмування на додаток до навичок системного адміністрування.

*Puppet* *Enterprise* має найповніший веб-інтерфейс з безлічі, що дозволяє в реальному часі керувати керованими вузлами за допомогою готових модулів і кулінарних книг, представлених на головних серверах. Веб-інтерфейс добре працює для управління, але не дозволяє налаштовувати модулі. Інструменти звітності добре розроблені, надаючи детальну інформацію про те, як поводяться агенти і які зміни були внесені.

З точки зору загальної концепції *Chef* схожий на *Puppet* в тому, що на керованих вузлах встановлені головний сервер і агенти, але він відрізняється в реальному розгортанні. Крім головного сервера, для установки *Chef* також потрібна робоча станція для управління головним сервером. Агенти можуть бути встановлені з робочої станції за допомогою ножового інструменту, який використовує *SSH* для розгортання, що полегшує установку. Після цього керовані вузли проходять перевірку автентичності за допомогою майстра з використанням сертифікатів.

Конфігурація *Chef* обертається навколо *Git*, тому знання того, як працює *Git*, є обов'язковою умовою роботи *Chef*. Як і *Puppet*, *Chef* заснований на *Ruby*, тому знання *Ruby* також необхідно. Як і в *Puppet*, модулі можуть бути завантажені або записані з нуля і розгорнуті на керованих вузлах після необхідної конфігурації.

На відміну від *Puppet*, у *Chef* поки немає добре сформованої функції *push*, хоча доступний бета-код. Це означає, що агенти повинні бути налаштовані на періодичну реєстрацію з майстром, і негайне застосування змін не представляється можливим.

Веб-інтерфейс для *Enterprise* *Chef* функціональний, але не надає можливості змінювати конфігурації. Він не такий повний, як веб-інтерфейс для *Puppet* *Enterprise*, в ньому відсутні функції звітності та інші функції, але він дозволяє здійснювати управління запасами і організацію вузлів.

Як і *Puppet*, *Chef* отримує вигоду з великої колекції модулів і конфігураційних рецептів, які в значній мірі залежать від *Ruby*. З цієї причини *Chef* добре підходить для інфраструктури, орієнтованої на розвиток.

*Ansible* набагато більше схожий на *Salt*, ніж на *Puppet* або *Chef*. Завдання *Ansible* - спростити і прискорити роботу, не вимагаючи установки агента вузла. Таким чином, *Ansible* виконує всі функції через *SSH*. *Ansible* побудований на *Python*, на відміну від *Ruby*, заснованого *Puppet* and *Chef*.

Установка *Ansible* може бути виконана через клон сховища *Git* на головний сервер *Ansible*. Після цього керовані вузли додаються в конфігурацію *Ansible*, а авторизовані ключі *SSH* додаються до кожного вузла, пов'язаного з користувачем, під яким буде запускатися *Ansible*. Після цього головний сервер *Ansible* може зв'язуватися з вузлом через *SSH* і виконувати всі необхідні завдання. Для роботи з операційними системами або збірками, які за замовчуванням не дозволяють кореневої доступ *SSH*, *Ansible* приймає облікові дані sudo для запуску команд від імені *root* в цих системах.

*Ansible* може використовувати *Paramiko*, реалізацію *Python* *SSH2* або стандартний *SSH* для зв'язку, але є також прискорений режим, який забезпечує швидшу і масштабну зв'язок.

*Ansible* можна запустити з командного рядка без використання файлів конфігурації для простих завдань, таких як перевірка працездатності служби або запуск оновлень і перезавантажень. Для більш складних задач конфігурація *Ansible* обробляється за допомогою синтаксису *YAML* в файлах конфігурації, які називаються *Playbooks*. *Playbooks* також може використовувати шаблони для розширення їх функціональності.

*Ansible* має набір модулів, які можна використовувати для управління різними системами, а також хмарної інфраструктурою, такий як *Amazon* *EC2* і *OpenStack*. Призначені для користувача модулі *Ansible* можуть бути написані практично на будь-якій мові, якщо вихідні дані модуля є допустимими *JSON*.

Веб-інтерфейс доступний для *Ansible* в формі *AnsibleWorks* *AWX*, але *AWX* не прив'язувати безпосередньо до *CLI*. Це означає, що елементи конфігурації, присутні в інтерфейсі командного рядка, які не будуть відображатися в веб-інтерфейсі, поки не буде виконано етап синхронізації. Ви можете використовувати включений інструмент синхронізації, щоб тримати їх у курсі, але його потрібно буде запускати за розкладом. Веб-інтерфейс сам по собі функціональний, але не так сповнений, як *CLI*, тому ви виявите, що працюєте між ними в загальному використанні або просто використовуєте *CLI*.

*Salt* схожий на *Ansible* в тому, що це інструмент на основі *CLI*, який використовує *push*-метод взаємодії з клієнтом. Його можна встановити через *Git* або через систему управління пакетами на майстрах і клієнтів. Клієнти відправляють запит на головний сервер, який при прийнятті на головному сервері дозволяє управляти цим міньйон.

*Salt* може спілкуватися з клієнтами через загальний *SSH*, але масштабованість значно поліпшується за рахунок використання клієнтських агентів, які називаються *minions*. Крім того, Salt включає в себе асинхронний файловий сервер для прискорення обслуговування файлів для міньйонів, що є частиною зосередженості Salt на високій масштабованості.

Як і в *Ansible*, ви можете давати команди minions безпосередньо з *CLI*, наприклад, для запуску служб або установки пакетів, або ви можете використовувати файли конфігурації *YAML*, звані «станами», для обробки більш складних завдань. Існують також «стовпи», які представляють собою набори даних, розташовані в центрі, до яких держави можуть звертатися під час роботи.

Ви можете запросити інформацію про конфігурацію - наприклад, версію ядра або відомості про мережевому інтерфейсі - у міньйонів безпосередньо з *CLI*. Міньйон можуть бути окреслені за допомогою елементів інвентаризації, званих «зернами», які спрощують видачу команд сервера певного типу, не покладаючись на налаштовані групи. Наприклад, в одному напрямку *CLI* ви могли б призначатися для кожного міньйон, який виконує певну версію ядра.

Як і *Puppet*, *Chef* і *Ansible*, *Salt* пропонує велику кількість модулів для роботи з конкретним програмним забезпеченням, операційними системами і хмарними сервісами. Призначені для користувача модулі можуть бути написані на *Python* або *PyDSL*. Salt пропонує управління *Windows* так само, як і *Unix*, але більше підходить для систем *Unix* і *Linux*.

Веб-інтерфейс *Salt*, *Halite*, дуже новий і не такий повний, як веб-інтерфейси для інших систем. Він пропонує перегляд журналів подій і статусу міньйонів, а також має можливість запускати команди для міньйонів, але мало ще. Цей інструмент знаходиться в стадії активної розробки і обіцяє значно покращитися, але в даний час він не містить помилок і помилок.

Найбільшою перевагою солі є її масштабованість і відмовостійкість. У вас може бути кілька рівнів майстрів, що призводить до багаторівневого розташуванню, яке одночасно розподіляє навантаження і збільшує надмірність. Майстри вгору за течією можуть контролювати майстрів вниз за течією і їх міньйон. Іншою перевагою є пірінгова система, яка дозволяє Міньйон задавати питання майстрам, які потім можуть отримувати відповіді від інших серверів, щоб завершити картину. Це може бути зручно, якщо необхідно виконати пошук даних в базі даних в реальному часі, щоб завершити настройку міньйон.

У той час як *Puppet* і *Chef* звернуться до розробників і магазинам, орієнтованим на розробку, *Salt* і *Ansible* набагато більш пристосовані до потреб системних адміністраторів. Простий інтерфейс *Ansible* і зручність використання вписуються в образ мислення системного адміністратора, і в магазині з великою кількістю систем *Linux* і *Unix* *Ansible* швидко і легко запускається прямо з воріт (таблиця 2.1).

Таблиця 2.1 – Порівняльна таблиця програмних додатків.



Salt - самий гладкий і міцний з чотирьох, і, як і Ansible, вона знайде відгук у системних адміністраторів. Salt, що володіє високою масштабованість і здатністю, обмежена тільки веб-інтерфейсом.

Puppet є найбільш зрілим і, ймовірно, найбільш доступним з чотирьох з точки зору зручності використання, хоча настійно рекомендується тверде знання Ruby. Puppet не так обтічно, як Ansible або Salt, і її конфігурація може іноді ставати візантійської. Puppet – найбезпечніша ставка для різнорідних середовищ, але ви можете знайти, що Ansible або Salt краще підходять для більшої або однорідної інфраструктури.

У Chef стабільна і добре продумана компоновка, і хоча вона не зовсім відповідає рівню Puppet з точки зору необроблених функцій, це дуже вдале рішення. Chef може створити найскладнішу криву навчання для адміністраторів, яким не вистачає значного досвіду програмування, але він може бути найбільш природним для адміністраторів, орієнтованих на розробку, і магазинів розробки.

## **Висновки до другого розділу**

У даному розділі автором було проаналізовано процеси автоматизованого налаштування та розгортання конфігурації мережевого обладнання.

Було виділено два методи для автоматизованого налаштування та розгортання серверної та мережевої інфраструктури:

* оркестрація;
* управління конфігурацією;

Оскільки саме вони з використанням певних модулів дають змогу автоматизувати процес налаштування конфігурації безпеки на мережевому обладнанні.

# **РОЗДІЛ 3 МОДЕЛЬ АВТОМАТИЗОВАНОГО НАЛАШТУВАННЯ КОНФІГУРАЦІЇ БЕЗПЕКИ МЕРЕЖЕВОГО ОБЛАДНАННЯ НА ОСНОВІ ПЗ ANSIBLE**

**3.1 Модулі для роботи з мережевим обладнання**

Глобально, модулі для роботи з мережевим обладнанням можливо розділити на дві частини:

1. Модулі для обладнання з підтримкою API.
2. Модулі для обладнання, яке працює тільки через CLI.

Якщо обладнання підтримує API, як наприклад, NXOS , то для нього створено велику кількість модулів, які виконують конкретні дії, по налаштуванню функціоналу. Наприклад, для NXOS створено понад 60 модулів.

Для обладнання, яке працює тільки через CLI, Ansible підтримує такі три типи модулів:

1. os\_command - виконує команди show;
2. os\_facts - збирає факти про пристрої;
3. os\_config - виконує команди конфігурації.

Відповідно, для різних операційних систем, будуть різні модулі. Наприклад, для Cisco IOS модулі будуть називатися:

1. ios\_command;
2. ios\_config;
3. ios\_facts.

Аналогічні три модуля доступні для таких ОС:

1. Dellos10.
2. Dellos6.
3. Dellos9.
4. EOS.
5. IOS.
6. IOS XR.
7. JUNOS.
8. SR OS.
9. VyOS.

При роботі з мережевим обладнанням є кілька параметрів в playbook, що потрібно міняти:

1. gather\_facts - треба відключити, так як для мережевого обладнання використовуються свої модулі збору фактів;
2. connection - управляє тим, як саме буде відбуватися підключення. Для мережевого обладнання необхідно встановити в local.

Тобто, для кожного сценарію (play), потрібно вказувати:

1. gather\_facts: false;
2. connection: local.

Приклад:

- name: Run show commands on routers

hosts: cisco-routers

gather\_facts: false

connection: local

У Ansible змінні можна вказувати в різних місцях, тому ті ж настройки можна вказати по-іншому.

Наприклад, в розділі про файли конфігурації розглядалося як відключити збір фактів за замовчуванням (файл ansible.cfg):

[defaults]

gathering = explicit

Такий варіант підходить в тому випадку, коли Ansible використовується більше для підключення до мережевих пристроїв (або, локальні playbook використовуються для підключення до мережного обладнання).

В такому випадку, потрібно буде навпаки явно включати збір фактів, якщо він потрібен.

Вказати, що потрібно використовувати локальне підключення, також можна по-різному.

В інвентарному файлі:

[cisco-routers]

192.168.100.1

192.168.100.2

192.168.100.3

[cisco-switches]

192.168.100.100

[cisco-routers:vars]

ansible\_connection=local

Або в файлах змінних, наприклад, в group\_vars / all.yml:

---

ansible\_connection: local

У наступних розділах буде використовуватися такий варіант:

---

- name: Run show commands on routers

hosts: cisco-routers

gather\_facts: false

connection: local

У реальному житті потрібно вибрати той варіант, який найбільш зручний для роботи.

**Аргумент provider**

Модулі, які використовуються для роботи з мережевим обладнанням, вимагають завдання кількох аргументів.

Для кожного завдання повинні бути вказані такі аргументи:

1. **host** - ім'я або IP-адреса віддаленого пристрою;
2. **port** - до якого порту підключатися;
3. **username** - ім'я користувача;
4. **password** – пароль;
5. **transport** - тип підключення: CLI або API. За замовчуванням – cli;
6. **authorize** - чи потрібно переходити в привілейований режим (enable, для Cisco);
7. **auth\_pass** - пароль для привілейованого режиму.

## **Висновки до третього розділу**

У третьому розділі автором запропоновано реалізація двох варіантів модулів для роботи з мережевим обладнання. Це це модуль для обладнання з підтримкою API та модуль для обладнання, яке працює тільки через CLI. Також наведені алгоритми налаштування програмних модулів.

Реалізація запропонованих автором пропозицій доволить підвищити рівень безпеки мережевого обладнання шляхом розроблення моделі автоматизованого налаштування параметрів безпеки на мережевому обладнанні.

**ВИСНОВКИ**

У кваліфікаційній роботі бакалавра автором вирішено актуальне завдання, що полягає в удосконаленні налаштування конфігурації безпеки мережевого обладнання. Для вирішення наведеного завдання автором була визначеена мета роботи - підвищення рівня безпеки шляхом розроблення моделі автоматизованого налаштування параметрів безпеки на мережевому обладнанні.

У першому розділі кваліфікаційгної роботи бакалавра автором було проведено аналіз існуючих загроз безпеки в інфокомунікаційних мережах сучасності. Визначено, що із зростанням рівня впровадження інформаційних технологій у життя особистості, суспільства і держави, зростає рівень небезпеки у кібернетичному просторі. На адекватне реагування викликам сучасності потреббує нарощення система заходів щодо протидії викликам у кіберпросторі. Розглянуті загальні тенденції у забезпеченні кібербезпеки на всіх рівнях. Систематизовані типи загроз для користувачів. Розглянуті їх властивості.

Проведене дослідження основних сучасних підходів для розгортання інфраструктури та було визначено що хмарний підхід є найбільш доцільним для розгортання інфраструктури. Розглянуто хмарні сервіси та їх методи розгортання інфраструктури, та було виділено що підхід інфраструктура як код є доцільним для автоматизації розгортання інфраструктури, оскільки він дає можливості змінної архітектури, та використовуючи системи для безперервної інтеграції дозволить мінімалізувати помилки в конфігурації архітектури.

Автором було проаналізовано процеси автоматизованого налаштування та розгортання конфігурації мережевого обладнання. Було виділено два методи для автоматизованого налаштування та розгортання серверної та мережевої інфраструктури: оркестрація; управління конфігурацією. Саме вони з використанням певних модулів дають змогу автоматизувати процес налаштування конфігурації безпеки на мережевому обладнанні.

Запропоновано модель системи автоматизованого розгортання та налаштування серверної та мережевої інфраструктури. Розглянуто взаємозв’язок між сервісами, архітектуру рішення та порядок роботи всієї системи в цілому. Практичне застосування запропонованої моделі для автоматизованого налаштування та розгортання серверного та мережевого обладнання, дозволить зменшити витрати часу на розгортання та налаштування інфраструктури.

Мета роботи досягнута.

# **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Богуш, В.М. Теоретичні основи захищених інформаційних технологій: навч. посіб. / В.М. Богуш, О.А. Довидьков, В.Г. Кривуца. – К.: ДУІКТ, 2010. – 454 с.
2. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с.
3. Бурячок В. Л. Соціальна інженерія як метод розвідки інформаційно-телекомунікаційних систем / В. Л. Бурячок, О. Г. Корченко, Л. В. Бурячок // Захист інформації. – 2012. – № 4(57). – С. 5–12.
4. Гайворонський, М. В. Безпека інформаційно-комунікаційних систем / М.В. Гайворонський, О.М. Новіков. – К.: Видавнича група ВНУ, 2009. – 608 с.
5. Довгань О. Д. Кібертероризм як загроза інформаційному суверенітету держави / О. Д. Довгань, В. Г. Хлань // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 49–53.
6. Грищук Р. В. Основи кібернетичної безпеки: монографія / Р. В. Грищук, Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника. – Житомир: ЖНАЕ, 2016. – 636 с.
7. Д. Даниленко, О. Смірнов, Є. Мелешко, "Дослідження методів виявлення вторгнень в телекомунікаційні системи та мережі", Системи озброєння і військова техніка, Х.: Харк. нац. ун-т Повітряних Сил ім. І. Кожедуба, № 1, С. 92-100, 2012.
8. І. Ю. Субач, “Шляхи удосконалення систем виявлення кібернетичних атак”, на Всеукр. наук.-практ. конф. Актуальні проблеми забезпечення інформаційної безпеки держави, Київ, 2014, с. 112.
9. Казакова, Н. Ф. Моніторинг інформаційних ресурсів в захищених інформаційних мережах [Текст] / Н. Ф. Казакова // Світ інформації та телекомунікацій : VII міжнар. наук.-техн. конф. студентства та молоді, 2010 р: Київ. – С. 165-168.
10. Котенко И.В, Степашкин М.В., Дойникова Е.В. Анализ защищенности автоматизированных систем с учетом социо-инженерных атак // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3. С. 40–57.
11. Котенко И.В., Саенко И.Б. Создание новых систем мониторинга и управления кибербезопасностью // 2014. Том 84. № 11. С. 993–1001.
12. Baranov A., Somov A., Spirjakin D., Akbari S., Passerone R. POCO: ‘Perpetual’ operation of CO wireless sensor node with hybrid power supply. Sensors and Actuators A: Physical 238:112-121, 2016.
13. Павлиш В. А. Основи інформаційних технологій і систем: Навчальний посібник. / Павлиш В. А., Гліненко Л. К. - Львів: Видавництво Львівської політехніки, 2013. − 500 с.
14. Скопа, О. О. Проблематика якості послуг інтернет-провайдерів / О. О. Скопа, С. Л. Волков, К. Б. Айвазова // Збірник наукових праць Одеської державної академії технічного регулювання та якості. – 2013. – № 1(2). – С. 27-31.
15. Соколов В.Ю. Iнформацiйнi системи i технологiї : Навч. посiб. / Соколов В.Ю. − К. : ДУIКТ, 2010. − 138 с.
16. Т. И. Булдакова, и А. Ш. Джалолов, “Выбор технологий Data Mining для систем обнаружения вторжений в корпоративную сеть”. Инженерный журнал: наука и инновации, № 11 (23), с. 1-14, 2013.
17. Ляпандра А.С. Підхід до узагальненого оцінювання ресурсів програмованих логічних інтегральних схем / А.С. Ляпандра // Електротехнічні та комп’ютерні системи. – К.:"Техніка", 2012. – №7. – С.92–96.
18. Сугоняк І.І. Модель системи підтримки прийняття рішень з оптимального керування життєвим циклом інноваційних проектів підприємств / І.І. Сугоняк // Вісник ЖДТУ. – Серія: технічні науки. – 2007. – № 43 (4). – С. 91-99.
19. Табунщик Г. В. Проектування, моделювання та аналіз інформаційних систем: Навчальний посібник / Г.В. Табунщик, Р.К. Кудерметов, А. В. Притула. – Запоріжжя : ЗНТУ, 2011. – 292 с.
20. Чумаченко, О. І., Горбатюк, В. С. “Нова модель штучного нейрону для побудови нейронних мереж у задачі апроксимації” Міжнародна науково-практична конференція «Інформаційні технології та комп’ютерне моделювання», (2018): 296-299.
21. А. В. Федорченко, Д. С. Левшун, А. А. Чечулин, И. В. Котенко Анализ методов корреляции событий безопасности в SIEM-системах. Ч. 1 Тр. СПИИРАН. 2016. Вып. 47. C. 5-27.