КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
Кафедра інженерії програмного забезпечення та кібербезпеки

Захищено на кафедрі інженерії програмного
забезпечення та кібербезпеки
«29» листопада 2021 р.
з оцінкою 94 бали (А)

Підпис членів комісії:
_____
_____
_____

КУРСОВА РОБОТА
з дисципліни
«БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ»
НА ТЕМУ:
«Розробка ПЗ захисту корпоративної мережі КНТЕУ від НСД»

Виконав: студент факультету
інформаційних технологій
3 курсу 12 групи
Фєфєлов Максим Андрійович

Науковий керівник:
професор кафедри інженерії програмного
забезпечення та кібербезпеки
Пашорін Валерій Іванович

КИЇВ 2021

Київський національний торговельно-економічний університет

Кафедра інженерії програмного забезпечення та кібербезпеки

КАРТКА

завдання та контролю за ходом виконання курсової роботи

1. Прізвище та ініціали студента Фєфєлов М.А.
2. Факультет Факультет інформаційних технологій (ФІТ)
3. Курс, група 3 курс 12 група
4. Форма навчання денна
5. Номер залікової книжки №34/19-297
6. Номер та назва теми курсової роботи Розробка ПЗ захисту корпоративної мережі КНТЕУ від НСД
7. Дата погодження теми з науковим керівником 15 вересня 2021
8. Дата затвердження плану роботи 15 вересня 2021
9. Дата подання виконаної роботи на кафедрі 18 листопада 2021
10. Дата захисту роботи 29 листопада 2021
11. Тему, план і строки прийняв до виконання _____
(підпис студента)
12. Науковий керівник Пашорін В.І. _____
(прізвище та підпис)

«29» листопада 2021 р.

Київський національний торговельно-економічний університет

Рецензія на курсову роботу (проект) і результат захисту

Студента **Фєфєлов Максим Андрійович**
3 курсу 12 групи факультету інформаційних технологій

Курсова робота (проект) з «Безпека інформаційних систем»
(назва навчальної дисципліни)

Тема Розробка ПЗ захисту корпоративної мережі КНТЕУ від НСД

Реєстраційний № 12-26, дата одержання 15 вересня 2021р.

Науковий керівник проф. Пашорін В.В.
(вчене звання, прізвище, ініціали)

Зміст рецензії

У курсовій роботі студента Фєфєлов М.А. на тему «Розробка ПЗ захисту корпоративної мережі КНТЕУ від НСД» зазначено актуальність дослідження, мету, об'єкт, предмет та задачі дослідження.
У першій частині курсової роботи студент розглянув питання про необхідність захисту інформації та засоби його забезпечення. У другому розділі автор описав моделі загрози та порушника. У третьому розділі студент подав ідею для програмного засобу інформаційної безпеки. В цілому, курсова робота студента Фєфєлов М.А. на тему «Розробка ПЗ захисту корпоративної мережі КНТЕУ від НСД» оформлена у відповідності до Вимог, може бути допущена до захисту та заслуговує на позитивну оцінку.

Допущено до захисту "18" листопада 2021 р.

Захист планується о 8:30 "29" листопада 2021 р.

(час)

кафедра інженерії програмного забезпечення та кібербезпеки

(місце роботи комісії)

_____

(підпис наукового керівника)

Курсова робота захищена “29” листопада 2021 р.
з оцінкою «94» бали (А)

(за шкалою КНТЕУ, національною шкалою та шкалою ЄКТС)

Комісія:

1. _____ Пашорін В.В.
(підпис) (прізвище, ініціали)

2. _____ Самойленко Ю.О.
(підпис) (прізвище, ініціали)

3. _____ Власенко Л.О.
(підпис) (прізвище, ініціали)

ЗМІСТ

ВСТУП

Майже на кожному підприємстві використовується комп'ютерна техніка. Її застосовують для багатьох задач: збирання, обробка та зберігання даних, керування промисловим обладнанням на фабриках та багато іншого. Заклади освіти (інакше кажучи: школи, ліцеї, гімназії, коледжі, університети тощо) також використовують комп'ютери. Та всередині кожного з цих закладів уся ця техніка з'єднується в єдину корпоративну обчислювальну мережу. Це дозволяє комп'ютерам обмінюватися даними різного характеру та призначення, а також дає доступ до певних ресурсів закладу, до яких ніщо інакше не має права мати доступ.

Безумовно, корпоративна комп'ютерна мережа — це зручно. Та ця зручність може приховувати в собі певний ризик несанкціонованого доступу (НСД) до комп'ютерів у мережі. Часто комп'ютери в лабораторіях й аудиторіях також підключаються до корпоративної мережі для розмежовування або полегшення доступу студентів до деяких ресурсів усередині мережі та/або в Інтернеті. Та неправильне налаштування політики безпеки у мережі може призвести до катастрофічних наслідків (у кращому ж випадку — неприємних). Так, студент, користуючись корпоративною мережею університету, може проникнути на комп'ютер і отримати інформацію, яку студенти не мають права знати (приклад: службові записки, відповіді до майбутніх екзаменів), інакше кажучи, порушити службову таємницю. І це тільки один із наслідків.

Одне з рішень цієї проблеми: розробка програмного мережевого екрану — фаєрволу (firewall) для запобігання НСД методом розмежовування доступу до комп'ютера від конкретних груп комп'ютерів у мережі.

Завдання курсової роботи: дослідження проблеми можливостей несанкціонованого доступу (НСД) до або всередині корпоративної мережі КНТЕУ.

Метою даної роботи є розробка програмного рішення для запобігання НСД до ресурсів (комп'ютерів) у мережі.

Об’єктом дослідження є запобігання НСД за допомогою розмежовування доступу вузлів та/або користувачів корпоративної мережі один до одного.

Предметом дослідження є мережевий фаєрвол, адаптований під особливості даної мережі.

Під час виконання проекту будуть побудовані моделі загрози та порушника та описаний принцип роботи програмного рішення захисту.

РОЗДІЛ 1.
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Коротка характеристика сфери діяльності Київського національного торговельно-економічного університету

Київський національний торговельно-економічний університет (КНТЕУ) є одним із провідних вищих навчальних закладів (ВНЗ) України. Згідно з його назвою, університет орієнтований на підготовку спеціалістів з економіки, торгівлі, маркетингу, фінансів тощо. Та окрім «основних» спеціальностей, університет також готує спеціалістів і з інших сфер: ресторанно-готельний і туристичний бізнес, менеджмент, право, інформаційні технології, дизайн тощо. Вищий навчальний заклад готує спеціалістів за освітніми програмами ступенів «Молодший бакалавр», «Бакалавр», «Магістр» тощо.

Окрім надання освіти студентам, КНТЕУ також співпрацює з роботодавцями для проходження студентами практики та допомоги їм у знаходженні роботи (розвитку кар'єри).

1.2. Характеристика інформації, що підлягає захисту

Діяльність КНТЕУ, як і будь-якого навчального закладу, базується на кругообігу інформації. Вона буває абсолютно різного призначення та характеру. Крім того, у КНТЕУ дані розрізняються за колом людей, які мають право отримувати та/або змінювати їх.

Інформація існує в різному вигляді: візуальному (письмовому, друкованому), усному, електронному.

До інформації, що підлягає захисту, у першу чергу належать дані різного призначення та характеру про студентів і працівників, що не повинні бути у відкритому доступі, у тому числі (список нижче не є вичерпним):

- звіти та дані про успішність студентів;
- екзаменаційні білети та відповіді до них;
- службові записки між працівниками університету;

- особисті документи студентів і працівників;
- списки академічних груп.

Тобто, таким чином, описується інформація, яку потрібно берегти від тих, хто не має права на її отримання.

Крім того, захищеними ще мають бути бази даних, які містять інформацію для веб-сайтів і системи дистанційного навчання. Загалом, захищеною має бути вся інформація, що стосується КНТЕУ та його студентів і працівників та його діяльності.

На жаль, захист інформації не є ідеальним. Існує кілька ризиків, що можуть призвести до витоку, спотворення або знищення інформації. Більшість з них криється в інформаційній інфраструктурі КНТЕУ; вона є слабким місцем у захисті інформації. Варто розглянути одну з її основних складових: корпоративну мережу університету.

1.3. Характеристика можливих заходів із захисту інформації

Було розглянуто один із вагомих ризиків безпеки для інформації всередині корпоративної мережі університету. Тепер потрібно розглянути можливі заходи із захисту інформації від несанкціонованого доступу (НСД).

Для запобігання несанкціонованому доступу до чуттєвої інформації в корпоративній мережі використовуються різні мережеві екрани, інакше кажучи фаєрволи (firewall). Даний засіб засновується на принципі фільтрування мережевого трафіку згідно з певною політикою безпеки — «правилами». Кожне з цих правил, наприклад, містить IP-адреси, протоколи та/або порти, пакети з яких потрібно відхиляти або пропускати.

Використання фаєрволів, програмних та/або апаратних, нарівні з правильним налаштуванням мережевого обладнання та комп’ютерів університету кваліфікованим технічним персоналом, повинно бути надійним рішенням проти НСД зсередини та ззовні корпоративної мережі.

Висновки до Розділу 1

У цьому розділі було описано коротку характеристику діяльності КНТЕУ. Найголовніше в цьому розділі є детальне роз’яснення причин захищати інформацію університету та приклади тих самих чуттєвих даних. Було детально описано експеримент, проведений для перевірки захищеності комп’ютерів у корпоративній мережі, результат і досвід, отриманий з нього.

Було описано можливі заходи із захисту інформації в корпоративній мережі від несанкціонованого доступу.

РОЗДІЛ 2.
АНАЛІЗ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ В КНТЕУ

2.1. Побудова моделі загроз

Для визначення оптимального способу та/або засобу захисту інформації в університеті, потрібно визначити модель загрози. У наступних розділах буде описаний експеримент, під час якого було виявлено цю загрозу, а нижче наводиться опис її моделі за певними параметрами:

- **Природа виникнення** — загроза є штучною.
- **Ступінь навмисності** — низький, бо «дірки» в системі безпеки створюються через людський фактор.
- **Безпосереднє джерело загроз** — людський фактор з боку технічного персоналу, який відповідає за налаштування інформаційних систем (ІС), та безпосередніх їхніх користувачів, які можуть випадково змінити їхні налаштування.
- **Міра залежності від активності ІС** — загроза існує, поки до вразливої інформаційної системи є доступ з корпоративної мережі.
- **Міра впливу на ІС** — загроза на самі ІС не впливає.
- **Етапи доступу користувачів або програм до ІС** — технічний персонал і користувачі (за умови, якщо вони мають доступ до адміністративного облікового запису на комп’ютері) мають безпосередній доступ до інформаційної системи.

Це було розглянуто загрозу інформаційній безпеці з боку працівників університету.

2.2. Побудова моделі порушника

Здебільшого типовим порушником безпеки інформаційних систем університету є студент. Модель порушника наведено далі:

- **Можлива мета порушника та її градація за ступенем небезпеки для ІС** — зазвичай порушник намагається проникнути в ІС або заради

самоствердження, або, скажімо, для отримання відповідей до своїх майбутніх екзаменів.

- **Категорія осіб, із яких може бути порушник** — студенти університету.
- **Можлива кваліфікація порушника** — щоб скористатися вразливістю, потрібно принаймні більш-менш добре «розбиратися в комп'ютерах».
- **Можливий характер його дій** — пошук у корпоративній мережі комп'ютерів з відкритим спільним доступом до файлів і принтерів.

2.3. Оцінювання ризику реалізації загроз у комунікаційних системах

Варто розглянути тут власний досвід, отриманий при перевірці захищеності корпоративної мережі університету. Передусім потрібно коротко описати сам об'єкт перевірки, а власне: корпоративну мережу КНТЕУ.

Університет складається з декількох будівель (корпусів), що знаходяться в різних частинах міста Києва. Кожна з цих будівель має доступ до корпоративної мережі, яка з'єднує між собою будівлі та комп'ютери всередині. Це дозволяє обмінюватися даними, наприклад, між комп'ютером у корпусі «А» та іншою ЕОМ у корпусі «М».

Експериментальним шляхом було виявлено один із таких ризиків. На значній кількості комп'ютерів було увімкнено видимість комп'ютера в «мережевому оточенні». Деякі з них мають увімкнений спільний доступ, що вимагають уведення імені користувача та паролю. А от на одному з таких комп'ютерів було виявлено значну загрозу витоку службової інформації внаслідок неправильного налаштування спільного доступу до папок і принтерів: файли одного з працівників університету, до яких ще належать службові документи, опинилися у вільному доступі з будь-якого комп'ютера, підключеного до корпоративної мережі.

Експеримент проводився, використовуючи комп'ютер в аудиторії.

2.4. Інженерно-технічні, апаратні та програмні засоби захисту інформації в КНТЕУ

Однією з ланок безпеки, яка існує в будь-якому разі, є операційна система та її службове програмне забезпечення на комп'ютерах університету. Вони відповідають за цілісність даних на цих інформаційних системах.

Визначення поточної конфігурації мережевого обладнання, установленого в університеті, на момент виконання курсової роботи було неможливим. Вважаймо, що на вході до корпоративної мережі з Інтернету встановлено певне захисне обладнання, яке захищає мережу від зовнішніх атак, захищає решту мережевого обладнання від перенапруги каналів зв'язку тощо.

Також вважається, що дії всередині корпоративної мережі КНТЕУ відстежуються. У випадок скоєння згубних учинків можна заглянути в журнал подій у мережі та визначити час події та місце, звідки було виконано ті чи інші дії.

Висновки до Розділу 2

Було побудовано модель загроз безпеці інформаційних систем КНТЕУ та побудовано модель порушника. У розділі детально описано експеримент із перевіркою захищеності інформаційних систем, а також наявність засобів безпеки.

Під час експерименту було виявлено значний ризик, що сприяє викраденню, спотворенню та/або знищенню даних зловмисниками на комп'ютерах університету. Комп'ютери, що видимі в «мережевому оточенні», якщо і мають увімкнений спільний доступ до файлів і принтерів з якоюсь метою, то доступ до них вимагає автентифікації. Проте, враховуючи наведені в описі експерименту можливі проблеми, що виникають при налаштуванні спільного доступу, можна дійти висновку, що повністю покладатися на політику безпеки в комп'ютерах не можна.

РОЗДІЛ 3.
ПРАКТИЧНА РЕАЛІЗАЦІЯ ДОДАТКОВИХ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ КНТЕУ

3.1. Наявність або відсутність служби з питань захисту інформації

Точний склад персоналу КНТЕУ не є відомим. Проте оскільки в університеті існує технічний персонал, який займається установкою та налаштуванням мережевого обладнання, можна припустити, що вони як раз є відповідальними за безпеку інформаційних систем.

На жаль, на момент написання роботи дослідження про службу з питань захисту інформації в навчальному закладі було неможливим. Та можна сказати точно, що в університеті є адміністратор системи дистанційного навчання, який відповідає за платформу Moodle та облікові записи MS Office 365 студентів і працівників.

3.2. Вибір, обґрунтування та опис функціонування додаткових програмно-апаратних засобів захисту інформації

Рішенням проблеми несанкціонованого доступу до інформаційних систем стане мережевий екран, або фаєрвол (firewall).

Здебільшого мережеві екрани для використання в корпоративних мережах існують як апаратні рішення. Підключення їх у будівлях університету — це модифікація вже існуючого обладнання, внесення змін у топологію мережі та/або інше. Установка захисного обладнання не завжди є можливою. Тому можливим варіантом залишається установка програмної реалізації фаєрволу.

Мережевий екран є програмним забезпеченням, що встановлюється на комп’ютери університету. Мають існувати декілька версій мережевого екрану: для серверів або персональних комп’ютерів, для різних операційних систем.

Варто розглянути мережевий екран для операційної системи на основі ядра Linux, оскільки відомо, що в цій ОС можна застосувати службове програмне

забезпечення (daemons), яке здатне керувати всім вхідним або вихідним мережевим трафіком; з комп’ютера можна навіть створити цілий маршрутизатор (router).

Отже, у програмі можна задати певну політику безпеки, згідно з якою мережевий екран має пропускати або не пропускати пакети/трафік. За замовчуванням можна не пропускати ніякий трафік, за винятком з комп’ютерів певних IP-адрес.

Відомо ще, що загальний доступ до папок у MS Windows використовує певні порти підключення. Тому потрібно мати можливість задати в політиці безпеки порти, які потрібно перекрити.

3.3. Розробка програмних модулів захисту інформації

Після дослідження проблеми, визначення способу її вирішення та визначення функціональності програмного рішення далі йде розробка ПЗ.

Оскільки маємо справу з програмним забезпеченням, що оперує мережевим трафіком, його потрібно писати мовою C або C++ для якнайбільшої продуктивності мережевого екрану та можливості прямого застосування системних API.

Щоб створити робочий прототип програмного фаєрволу однією людиною, на це могло б знадобитися багато часу.

Висновки до Розділу 3

Було визначено додаткові засоби захисту інформаційних систем від загроз. Опираючись на умови їхнього розгортання, приймається рішення про розробку програмного мережевого екрану для фільтрації трафіку всередині корпоративної мережі КНТЕУ.

Мережевий екран КНТЕУ має бути комплексним програмним рішенням, тому в даній курсовій роботі лише описано принцип його роботи.

ВИСНОВКИ

Під час виконання даної роботи було досліджене питання захисту корпоративної мережі КНТЕУ. Було визначено приблизний перелік даних, що вимагають захисту від несанкціонованого доступу (НСД) всередині та ззовні мережі. Експериментальним шляхом перевірено захищеність корпоративної мережі КНТЕУ та виявлено вразливості. Визначено моделі загроз і порушника. Усі ці фактори є привидом створення мережевого екрану, адаптованого під особливості цієї обчислювальної мережі.

Було описано принцип роботи мережевого екрану власної розробки на прикладі електронно-обчислювальної машини з операційною системою Linux.

Безумовно, задумка, описана у принципі роботі цього рішення, дуже непогана. Та щоб створити робочий прототип однією людиною, на це знадобиться багато часу.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Офіційний сайт Київського національного торговельно-економічного університету. [Електронний ресурс] https://knute.edu.ua/
2. Півень А.Г., Шевченко І.П. Захист інформації та використання інформаційних технологій в інтелектуальній власності. [Електронний ресурс] https://core.ac.uk/download/pdf/324244299.pdf (дата звернення 25.11.2021)
3. CompTIA Security+ SY0-501 Cert Guide, Academic Edition, 2nd Edition By David L. Prowse
4. Lance Spitzner. Honeypots: Tracking Hackers. Addison Wesley, 2002.
5. Stapelberg R.G. Handbook of Reliability, Availability, Maintainability and Safety in Engineering Design. Springer-Verlag London Limited, 2009.
6. Crimes R.A. Honeypots for Windows. - APRESS, 2005.
7. Klein M.H. A Practitioner's Handbook for Real-Time Analysis / Mark H. Klein, Thomas Ralya, Bill Pollak, Ray Obenza. - KIuwer Academic Publishers, 1993.
8. Diogenes Y. Cybersecurity - Attack and Defense Strategies / Yuri Diogenes, Erdal Ozkaya. - Packt Publishing Ltd., Livery Place,35 Livery Street, Birmingham, B3 2PB, UK, 2018.