

Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Навчально-науковий інститут цивільного захисту
Кафедра управління інформаційною безпекою

«Допущено до захисту»
Начальник кафедри УІБ
д.т.н. доц. Ткачук Р.Л.

“ _____ ” _____ 2021 року

ДИПЛОМНА РОБОТА БАКАЛАВРА

на тему Аналіз загроз інформаційної безпеки і захист даних об'єкту типу
“розумний дім”

Виконав:

студент 4 курсу,
групи КБ-41, спеціальності 125
«Кібербезпека»

(шифр і назва спеціальності)

Назарій ДАЦКІВ

(прізвище, ім'я, по батькові)

Керівник Орест ПОЛОТАЙ

(прізвище та ініціали)

Рецензент Богдан МІЗЮК

(прізвище та ініціали)

Львів – 2021 року

АНОТАЦІЯ

Назарій ДАЦКІВ «Аналіз загроз інформаційної безпеки і захист даних об'єкту типу «розумний дім». Дипломна робота за спеціальністю 125 «Кібербезпека» складається з текстової частини, що містить 3 розділи, 60с., 26 рисунків, 14 таблиць, 20 джерел.

Об'єктом дослідження є система «розумний дім» як сукупність програмно-апаратних засобів підтримки інформаційних технологій для забезпечення комфортного та безпечного проживання громадян.

Мета роботи – підвищення захищеності ІТ-систем «розумного будинку» шляхом дослідження загроз і вразливостей інформаційної безпеки «розумного будинку», а також застосування натурального моделювання для перевірки працездатності пропонованих рішень щодо захисту «розумного будинку».

Методи дослідження – вивчення наукової літератури з теми дослідження, нормативно-правової бази, аналітичний і порівняльний методи, методи системного аналізу.

У першому розділі розглянуті основні типи систем «розумного будинку», розглянуті і проаналізовані уразливості для використовуваних програмно-апаратних засобів в таких системах. У другому розділі проводиться оцінка ризиків інформаційної безпеки для «розумного будинку», розроблені рекомендації по вибору і опису захисних заходів щодо зниження ризиків реалізації загроз інформаційної безпеки. Третій розділ присвячений дослідженню прототипу фрагмента системи «розумний дім» та його захищеності.

ЗАХИСТ ІНФОРМАЦІЇ, РОЗУМНИЙ БУДИНОК, РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

ABSTRACT

Nazarij DATSKIV "Analysis of information security threats and data protection of the object such as "smart home". Thesis in the specialty of 125 "Cybersecurity" consists of textual part that contains 3 sections, 60 pages, 26 figures, 14 tables, 20 sources.

The object of the study is the system "smart home" as a set of software and hardware to support information technology to ensure comfortable and safe living for citizens.

The purpose of the work is to increase the security of IT systems of the "smart home" by studying the threats and vulnerabilities of information security of the "smart home", as well as the use of field modeling to test the proposed solutions to protect the "smart home".

Research methods - the study of scientific literature on the research topic, regulatory framework, analytical and comparative methods, methods of systems analysis.

The first section discusses the main types of "smart home" systems, discusses and analyzes vulnerabilities for the software and hardware used in such systems. The second section assesses the risks of information security for the "smart home", developed recommendations for the selection and description of protective measures to reduce the risks of information security threats. The third section is devoted to the study of the prototype fragment of the system "smart home" and its security.

**INFORMATION PROTECTION, REASONABLE HOUSE,
INFORMATION SECURITY RISKS**

ЗМІСТ

ВСТУП	6
Розділ 1. ДОСЛІДЖЕННЯ ОСНОВНИХ ХАРАКТЕРИСТИК «РОЗУМНОГО БУДИНКУ» ЯК ОБ'ЄКТА ЗАХИСТУ	8
1.1. Основні положення по організації системи «розумного будинку»	8
1.2. Дослідження характеристик основних підсистем «розумного будинку»	12
1.3. Аналіз вразливостей і факторів, що впливають на датчики контролю і захисту в системі «розумний дім»	16
1.4. Аналіз вразливостей і факторів, що впливають на виконавчі пристрої «розумного будинку»	22
1.5. Аналіз вразливостей і факторів, що впливають на безпеку центральних пристроїв «розумного будинку»	23
1.6. Аналіз вразливостей і факторів, що впливають на систему зв'язку «розумного будинку»	26
Висновки до розділу	31
Розділ 2. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ «РОЗУМНОГО БУДИНКУ»	31
2.1. Загрози конфіденційності, цілісності та доступності інформації ІТ-системи «розумного будинку»	32
2.2. Оцінка ризиків інформаційної безпеки «розумного будинку»	34
Висновки до розділу	38
Розділ 3. ДОСЛІДЖЕННЯ ЗАХИЩЕНОСТІ ПРОТОТИПУ ФРАГМЕНТА СИСТЕМИ «РОЗУМНИЙ ДІМ»	39
3.1. Загальний опис запропонованого прототипу фрагмента системи «розумний дім»	39
3.2. Способи реалізації прототипу системи «розумний будинок»	43
3.3. Практичне дослідження захищеності запропонованого пристрою	46
3.4. Поради, щодо захисту «розумного будинку»	48
Висновки до розділу	57
ЗАГАЛЬНІ ВИСНОВКИ	58
ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ	59

ЗАГАЛЬНІ ВИСНОВКИ

Мета цієї дипломної роботи полягала в дослідженні захищеності ІТ-систем «розумного будинку» шляхом виявлення загроз і вразливостей інформаційної безпеки «розумного будинку», а також застосування натурального моделювання для перевірки працездатності пропонованих рішень щодо захисту «розумного будинку».

Для досягнення зазначеної мети в ході виконання дипломної роботи були вирішені наступні завдання:

1) під час вирішення завдання вивчення основних типів і характеристик систем «розумного будинку», були виявлені їх ключові уразливості. Також проведено дослідження вразливостей апаратного забезпечення систем «розумного будинку»;

2) проведена якісна оцінка ризиків інформаційної безпеки «розумного будинку» і вироблені захисні заходи для їх зниження;

3) досліджено прототип фрагмента системи «розумний дім» на базі плати Arduino Uno SMD;

4) при експериментальному дослідженні загроз і вразливостей розробленого прототипу фрагмента системи «розумний дім» була детально вивчена загроза перехоплення критично важливої інформації системи. Після чого на підставі теоретичної частини дослідження, були вироблені рекомендації для усунення даної уразливості.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Баранников, Н. И. Моделирование угроз информационной безопасности АСУЗ с помощью SWOT-анализа [Текст] / Н. И. Баранников, В. В. Лукин // Молодой ученый. – 2016. – №4. – С. 19-22.
2. Бурнашов С. В. Проектування та розроблення відкритих wifi-мереж з функцією збирання інформації про пристрої / С. В. Бурнашов, Ящук В. І. // Інформаційна безпека та Інформаційні технології: збірник тез доповідей IV Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів, м. Львів, 27 листопада 2020 року. Львів, ЛДУ БЖД, 2020, 249 с. (С.121-124).
3. Васильев, А. И. Проблемы защиты информации в интернете вещей [Текст] / А. И. Васильев, А. Ю. Гребешев // XVII Междунар. науч.-техн. конф. «Проблемы техники и технологий телекоммуникаций» тр. конф. – Самара, 2016. – С. 191-192.
4. Войтович В.С., Гриник Р.О. Необхідність створення комплексної системи захисту інформації. Зб. тез доповідей II Міжвузівської науково-практичної конференції студентів і курсантів “Захист інформації в інформаційно-комунікаційних системах” (м. Львів, 24 листопада 2017 р.). Львів: ЛДУ БЖД, 2017. С. 10–11.
5. Войтович В.С., Гриник Р.О. Дослідження проблематики кібербезпеки України Зб. наук. праць XII Міжнар. наук.-практ. конф. молодих вчених, курсантів та студентів “Проблеми та перспективи розвитку системи безпеки життєдіяльності” (м. Львів, 23-24 березня 2017 р.). [в 2 ч.]. Ч. 2. – Львів: ЛДУ БЖД, 2017. С. 11–12.
6. Войтович В.С., Гриник Р.О. Основні безпекові проблеми кіберпростору України. Зб. тез доповідей Міжнародна науково-практична конференція “Інформаційна безпека в сучасному суспільстві” (м. Львів, 24-25 листопада 2016 р.). Львів : ЛДУБЖД, 2016. С. 23–24.
7. Заник О., Ткачук Р. Вплив людського фактору на системи організації інформаційної безпеки. Зб. тез доповідей V Всеукр. наук.-практ конф. молодих

учених, студентів і курсантів “Інформаційна безпека та інформаційні технології” (м. Львів, 26 листопада 2020 р.). Львів : ЛДУБЖД, 2020. С. 21–22.

8. Защита информации в компьютерных сетях. Практический курс. [Текст] : учеб. пособие / ред.: Н. И. Синадский. – Екатеринбург: УГТИ-УПИ, 2008. - 248 с.

9. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения [Текст] : ГОСТ Р 53114-2008. – Введ. 2009-10-01.

10. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения [Текст] : ГОСТ Р 51275 – 2006. - Введ. 2008-02-01. -

11. Интернет вещей [Текст] / ред. А. В. Росляков. – Самара: ИУНЛ ПГУТИ, 2014. – 342 с.

12. Информационная технология. Методы обеспечения безопасности. Менеджмент безопасности информационных и телекоммуникационных технологий. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий [Текст] : ГОСТ Р ИСО/МЭК 13335-1-2006 – Введ. 2007-08-01.

13. Малыш, В. Н. Анализ угроз информационной безопасности системы «Умный дом» [Текст] / В. Н. Малыш, Д. С. Букреев // Труды Международного симпозиума «Надежность и качество». – 2012. Т. 1, – С. 149

14. Н.Дацків, О.Полотай Загрози конфіденційності, цілісності та доступності інформації ІТ-системи «розумного будинку». Автоматизація та комп'ютерно-інтегровані технології у виробництві та освіті: стан, досягнення, перспективи розвитку: матеріали Всеукраїнської науково-практичної Internet-конференції. – Черкаси, 2021. - С.49-50. 1.

15. Снегуров, А. В. Риски информационной безопасности систем, построенных по технологии «Умный дом» [Текст] / А. В. Снегуров, Е. А. Ткаченко, А. Д. Кравченко // Восточно-Европейский журнал передовых технологий. – 2011. – № 3(52). – С. 30-34.

16. Таненбаум Э., Компьютерные сети [Текст] / Э. Таненбаум, Д. Уэзеролл. -5-е изд. – СПб: Питер, 2012. -960 с.

17. Ящук В. І. Онтологія наукових досліджень та методологія наукового пізнання / В.І. Ящук // Економіка в контексті глобальних змін суспільства: матеріали Міжнародної науково-практичної конференції (м. Дніпро, 18 липня 2020 р.). – Дніпро: НО «Перспектива», 2020. – 140 с. (С.100-104).

18. <https://klaster.ua/ua/stati-i-obzory/kak-zaschitit-umnyy-dom-ot-hakerov/>

19. O.Polotai, O. Belej., N. Nestor, S. Panchak Developing a Model of Cloud Computing Protection System for the Internet of Things. 2020 IEEE 16th International Conference on the Perspective Technologies and Methods in MEMS Design, MEMSTECH 2020 - Proceedings, 2020, pp. 53-58

20. O.Polotai, O.Belej, K.Kolesnyk Application of neural networks in intrusion monitoring system for wireless sensor networks. Conference on computer science and information technologies. CSIT 2020: advances in intelligent systems and computing, vol 1293, Springer, Cham. – pp.1101-1115.