**Міністерство освіти і науки України**
**Національний технічний університет**
**«Дніпровська політехніка»**

**Інститут електроенергетики**
**Факультет інформаційних технологій**
**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеню магістра

**студента** ***Гриба Михайла Олексійовича***

**академічної групи** ***125м-17-1***

**спеціальності** ***125 Кібербезпека***

**спеціалізації**[1] ***Кібербезпека***

**за освітньо-професійною програмою** ***Кібербезпека***

**на тему** ***Аналіз ефективності елементів модуля «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х***

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | д.т.н., проф. Корнієнко В.І. | | | |
| розділів: | | | | |
| спеціальний | ст.викл. Кручінін О.В. | | | |
| економічний | к.е.н., доц. Пілова Д.П. | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент** | | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | ст. викл. Мєшков В.І. | | | |

**Дніпро**
**2018**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

# ЗАВДАННЯ
## на кваліфікаційну роботу ступеня магістра

**студенту** ***Гриб Михайло Олексійович*** **академічної групи** ***125М-17-1***
(прізвище та ініціали) (шифр)

**спеціальності** ***125 Кібербезпека***

**спеціалізації**[1] ***Кібербезпека***

**за освітньо-професійною програмою** ***Кібербезпека***

**на тему** ***Аналіз ефективності елементів модуля «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х***

**1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ**

Наказ ректора НТУ «Дніпровська політехніка» від 29.11.18 № 2025-л_____

**2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ**

**Об'єкт досліджень** ***модуль «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х***

**Предмет досліджень** ***ефективність модуля «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х***

**Мета** ***створення умов для оцінки відповідності вимогам НД ТЗІ та експертизи систем захисту які використовують програмний засіб «Бітрікс: Управління сайтом» версії 18.х***

**Вихідні дані для проведення роботи** ***матеріали науково – дослідної та преддипломної практик***

**3 ОЧІКУВАНІ РЕЗУЛЬТАТИ**

**Наукова новизна** ***розробка програми та методики проведення аналізу рівня захищеності системи «Бітрікс: Управління сайтом» версії 18.х***

**Практична цінність** ***зменшення часу та фінансових витрат при проведенні захищеності та експертизи систем***

## 4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

***Відповідність методичним рекомендаціям до підготовки та захисту дипломної роботи та вимогам нормативним документів з технічного захисту інформації***

## 5 ЕТАПИ ВИКОНАННЯ РОБІТ

| **Найменування етапів робіт** | **Строки виконання робіт** (початок-кінець) |
|---|---|
| Огляд джерел за темою та напрям досліджень | 03.09.18-06.10.18 |
| Методи досліджень | 07.10.18-31.10.18 |
| Результати досліджень | 01.11.18-24.11.18 |
| Виконання економічного розділу | 25.11.18-04.12.18 |
| Оформлення пояснювальної записки | 05.12.18-10.12.18 |

## 6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект** ***запобігання фінансових витрат у разі спроби атаки на веб-додаток***

**Соціальний ефект** ***підвищення рівня кібербезпеки веб - додатків***

## 7 ДОДАТКОВІ ВИМОГИ

**Завдання видано** _____ _____
(підпис керівника) (прізвище, ініціали)

**Дата видачі: 03.09.18р.**

**Дата подання до екзаменаційної комісії: 14.12.18р.**

**Прийнято до виконання** _____ _____
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: с., рис., табл., додатків, джерел.

Об’єкт дослідження: модуль «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х.

Мета роботи: створення умов для оцінки відповідності вимогам НД ТЗІ та експертизи систем захисту які використовують програмний засіб «Бітрікс: Управління сайтом» версії 18.х.

Метод дослідження – аналіз і випробування.

У спеціальній частині доведено виконання функціональних послуг безпеки за допомогою елементів модуля «Проактивний захист».

У роботі проведено аналіз популярних систем управління вмістом сайту (CMS), обгрунтовано вибір системи «Бітрікс: Управління сайтом» версії 18.х, як об’єкта досліджень. Проведено експертизи елементів модуля «Проактивний захист», на основі якої визначено, які функціональні послуги безпеки вони реалізують.

В економічному розділі наведено обгрунтування запропонованої програми та методики.

Практичне значення роботи полягає у зменшенні часу та фінансових витрат при проведенні експертизи захищеності систем. Результати здійснених у дипломній роботі досліджень можуть бути використані для проведення експертизи систем захисту з використанням системи «Бітрікс: Управління сайтом» версії 18.х.

Наукова новизна дослідження полягає у розробці програми та методики проведення аналізу.

Напрямки подальших досліджень полягають у перевірці інших функціональних послуг безпеки, що не були розглянуті у даній роботі.

CMS, ВЕБ – ДОДАТОК, ВРАЗЛИВІСТЬ, ПРОГРАМА, МЕТОДИКА, ЕКСПЕРТИЗА, ПОСЛУГА БЕЗПЕКИ.

# РЕФЕРАТ

Пояснительная записка с., рис., табл., приложений, источников.

Объект исследования: модуль «Проактивная защита» системы «Битрикс: Управление сайтом» версии 18.х.

Цель работы: создание условий для оценки соответствия требованиям НД ТЗИ и экспертизы систем защиты. которые используют программное средство «Битрикс: Управление сайтом» версии 18.х.

Метод исследования – анализ и испытание.

В специальной части доказано выполнение функциональных услуг безопасности с помощью элементов модуля «Проактивная защита».

В работе проведен анализ популярных систем управления содержимым сайта (CMS), обоснован выбор системы «Битрикс: Управление сайтом» версии 18.х, как объекта исследований. Проведено экспертизы элементов модуля «Проактивная защита», на основе которой определено, какие функциональные услуги безопасности они реализуют.

В экономическом разделе приведены обоснования предложенной программы и методики.

Практическое значение работы состоит в уменьшении времени и финансовых затрат при проведении экспертизы защищенности систем. Результаты проведенных в дипломной работе исследований могут быть использованы для проведения экспертизы систем защиты с использованием системы «Битрикс: Управление сайтом» версии 18.х.

Научная новизна исследования заключается в разработке программы и методики проведения анализа.

Направления дальнейших исследований заключаются в проверке других функциональных услуг безопасности, которые не были рассмотрены в данной работе.

ВЕБ – ПРИЛОЖЕНИЕ, CMS, УЯЗВИМОСТЬ, ПРОГРАММА, МЕТОДИКА, ЭКСПЕРТИЗА, УСЛУГА БЕЗОПАСНОСТИ.

# ABSTRACT

Explanatory note p., pic., tables., applications, sources.

Object of research: the module "Proactive Defense" of Bitrix: Site Management system, version 18.x.

Purpose of the work: the creation of conditions for assessing compliance with the requirements of Sun TSI and the examination of security systems using Bitrix Sitemaps program version 18.x.

Method of research - analysis and testing.

The special part demonstrates the implementation of functional security services through the elements of the module "Proactive Defense".

The analysis of popular site content management systems (CMS) has been carried out, substantiating the choice of "Bitrix Site Management" system version 18.x as an object of research. Examination of the elements of the module "Proactive Defense" was conducted, providing a basis to determine what functional safety services the elements implement.

The economic section provides justification for the proposed program and methodology.

The practical value of the work is to reduce the time and cost of conducting an examination of a security system. The results of the thesis research work can be used for examination of security systems by using Bitrix: Site Management version 18.x.

The scientific novelty of the study is to develop a program and methodology for conducting the analysis.

The direction of further research is to check other functional security services that were not addressed in this paper.

CMS, WEB APPLICATION, VULNERABILITY, THREAT, PROGRAM, METHOD, EXAMINATION, SECURITY SERVICE.

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

API (Application Programming Interface) – прикладний програмний інтерфейс;

CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) – повністю автоматизований публічний тест Тюринга для розрізнення комп'ютерів і людей;

CMS (Content Management System) – система керування вмістом;

CSS (Cascading Style Sheets) – каскадні таблиці стилей;

DDoS (Distributed Denial of Service) – розподілена атака на відмову в обслуговуванні;

HTML (Hypertext Markup Language) – мова гіпертекстової розмітки;

HTTP (Hypertext Transfer Protocol) – протокол передачі гіпертексту;

IEC (International Electrotechnical Commission) – міжнародна комісія з електротехніки;

ISO (International Organization for Standardization) – міжнародна організація по стандартизації;

IP (Internet Protocol) – міжмережевий протокол;

IT (Information technology) – інформаційні технології;

LDAP (Lightweight Directory Access Protocol) – полегшений протокол доступу до директорій;

OS (operating system) – операційна система;

OTP (One Time Password) – Одноразовий пароль;

OWASP (Open Web Application Security Project) – відкритий проект забезпечення безпеки веб-додатків;

PHP (Hypertext Preprocessor) – препроцесор гіпертексту;

RFI (Remote File Inclusion) – віддалене виконання файлів;

RSA (абревіатура від прізвищ Rivest, Shamir та Adleman) – криптографічний алгоритм з відкритим ключем;

SQL (Structured Query Language) – мова структурованих запитів;

SSL (Secure Sockets Layer) – рівень захищених сокетів;

WAF (Web Application Firewal) – Брандмауер веб-додатків;

WASC (Web Application Security Consortium) – Консорціум безпеки веб – додатків;

XML (eXtensible Markup Language) – розширювана мова розмітки;

XSS (Cross – site Scripting) – міжсайтове иконання сценаріїв;

КС - комп’ютерна система;

НД ТЗІ – нормативний документ системи технічного захисту інформації.

ЗМІСТ

С.

# ВСТУП

Сфера застосування веб-технологій розширюється з кожним роком. Більшість компаній використовує у своїй діяльності веб-додатки для роботи з клієнтами, забезпечення внутрішніх бізнес-процесів. І якщо функціональності веб-додатків приділяється значна увага, то питання їх безпеки часто вирішуються в останню чергу, що негативним чином позначається на рівні захищеності всього підприємства.

Вразливості веб-додатків надають зловмисникам широкий простір для дій. Помилки проектування і адміністрування дозволяють атакуючим отримувати важливу інформацію, а також порушувати функціонування веб-додатки, здійснювати атаки на відмову в обслуговуванні, проводити атаки на користувачів, проникати у внутрішню мережу компанії і отримувати доступ до критично значущим ресурсів.

Об’єкт дослідження: модуль «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х.

Мета роботи: створення умов для оцінки відповідності вимогам НД ТЗІ та експертизи систем захисту які використовують програмний засіб «Бітрікс: Управління сайтом» версії 18.х.

У роботі проведено аналіз найпопулярніших CMS, доцільності використання системи «Бітрікс: Управління сайтом» версії 18.х., а також аналіз ефективності елементів модуля «Проактивний захист».

Практичне значення роботи полягає у зменшенні часу та фінансових витрат при проведенні експертизи захищеності систем.

Наукова новизна дослідження полягає у розробці програми та методики проведення аналізу рівня захищеності системи «Бітрікс: Управління сайтом» версії 18.х.

# РОЗДІЛ 1. АНАЛІЗ ВРАЗЛИВОСТЕЙ ВЕБ-ДОДАТКІВ. АНАЛІЗ CMS. ОГЛЯД СИСТЕМИ «БІТРІКС: УПРАВЛІННЯ САЙТОМ» ВЕРСІЇ 18.X.

## 1.1 Аналіз функціонування веб – додатків та технологій їх побудування

Веб-додаток – клієнт - серверний додаток, в якому клієнтом виступає браузер, а сервером - веб-сервер. Логіка веб-додатка розподілена між сервером і клієнтом, зберігання даних здійснюється, переважно, на сервері, обмін інформацією відбувається по мережі. Одним з переваг такого підходу є той факт, що клієнти не залежать від конкретної операційної системи користувача, тому веб-додатки є міжплатформними сервісами.

Веб-додаток складається з клієнтської і серверної частин, тим самим реалізуючи технологію «клієнт-сервер».

Клієнтська частина реалізує інтерфейс користувача, формує запити до сервера і обробляє відповіді від нього.

Серверна частина отримує запит від клієнта, виконує обчислення, після цього формує веб-сторінку і відправляє її клієнту через мережу з використанням протоколу HTTP. [1]. Принцип роботи веб – додатка представлено на функціональній схемі на рисунку 1.1.

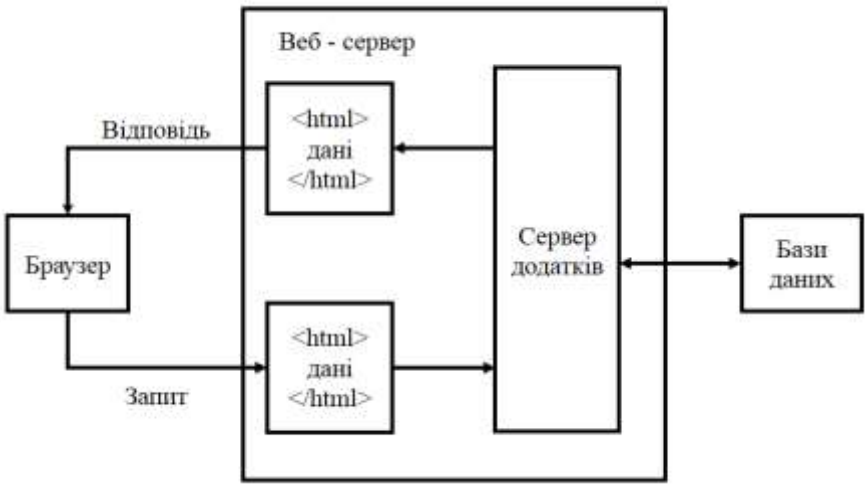



Рисунок 1.1 – Узагальнена функціональна схема веб – додатка

Браузер виконує запит до веб-сервера, веб-сервер находить сторінку і передає її серверу додатків. Сервер додатків переглядає сторінку на наявність інструкцій і виконує її підготовку, потім відправляє запит базі даних. База даних відправляє відповідь. Сервер додатків вставляє дані в сторінку і передає сторінку веб-серверу. Веб-сервер, який є програмним забезпеченням, відправляє підготовлену сторінку браузеру.

Для побудови серверної та клієнтської частин додатка використовуються різні мови програмування та технології. Код серверної частини, що обробляє запити клієнта, може бути реалізований за допомогою мов програмування [2]:

– Ruby on Rails;
– PHP;
– C#;
– Java;
– Python;
– JavaScript.

На стороні клієнта використовуються [2]:

– таблиці стилей CSS;
– мова гіпертекстової розмітки HTML;
– мова програмування JavaScript.

Слід зазначити, що веб-додатки функціонують в автоматизованих системах класу 2 та 3. Це визначає як їх вразливості, так і вимоги щодо їх захисту. Вимоги щодо захисту веб-сторінок наведену у НД ТЗІ 2.5-010 «Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу»[3].

## 1.2 Етапи розробки веб-додатків

Основними етапами розробки веб-додатків є [4]:

– Розробка технічного завдання. Складання документації, детально описує структурну і поведінкову моделі проекту.

– Створення дизайну та навігації. Детальне промальовування і визначення позиціонування, типових структурних елементів проекту.

– Верстання. Опис типових структурних елементів проекту на мові розмітки, відповідно до заданої специфікації.

– Програмування. Опис структурної та поведінкової моделей проекту на мовах програмування.

– Установка. Копіювання проекту на робочий сервер і інсталяція.

– Тестування та налагодження. Виявлення синтаксичних і логічних помилок проекту і подальше їх усунення.

Реалізація етапів розробки веб-додатків виконується послідовно. Етапи реалізуються зазвичай різним персоналом. Технічним завданням займається менеджер проекту, створенням дизайну – дизайнер, верстанням проекту – верстальник, програмуванням – програміст.

## 1.3 Аналіз вразливостей веб-додатків

Згідно з НД ТЗІ 1.1 – 003 – 99, вразливість системи – це нездатність системи протистояти реалізації певної загрози або сукупності загроз[5]. У стандарті ISO/IEC 29147:2014 Information technology. Security techniques. Vulnerability disclosure сказано, що вразливість – це слабкість програмного, апаратного забезпечення, або онлайн-сервісу, якою можна скористатися[6].

Одним з варіантів класифікації вразливостей та ризиків веб – додатків є рейтинг 10 найпоширеніших вразливостей та ризиків – OWASP Top – 10 – 2017. OWASP – це некомерційна благодійна організація, що займається підвищенням безпеки програмного забезпечення[7]. Остання редакція документа OWASP Top – 10 – 2017 виглядає наступним чином [8]:

– ін'єкції, (Injection) такі як SQL, NoSQL, OS та ін'єкції LDAP, виникають, коли ненадійні дані надсилаються інтерпретатору як частина команди або запиту. Ворожі дані атакуючого можуть змусити інтерпретатора

виконувати ненавмисні команди або отримувати доступ до даних без належного дозволу;

– некоректна автентифікація (Broken Authentication) – функції, пов'язані з автентифікацією та управлінням сеансами, часто виконуються неправильно, дозволяючи зловмисникам компрометувати паролі, ключі або сеансові токени, або використовувати інші недоліки, щоб отримати ідентифікатори користувачів;

– витік критичних даних (Sensitive Data Exposure) – багато веб-програм і API можуть не належним чином захищати критичні дані. Зловмисники можуть викрасти або модифікувати слабо захищені дані для здійснення шахрайства з кредитними картками, для крадіжки особистих даних або інших злочинів. Повинні вживатись спеціальні запобіжні заходи для критичних данних при обміні з браузером;

– атаки на засоби аналізу XML – вводу (XML Eternal Entities) – зловмисники можуть завантажувати XML – файли на сервер або включати шкідливий код у документ XML;

– неправильний контроль доступу (Broken Access Control) – контроль доступу реалізовано таким чином, що авторизовані користувачі можуть мати в системі повноваження, які не повинні мати. Зловмисники можуть використовувати цей недолік для доступу до неавторизованих функцій та / або даних, таких як доступ до облікових записів інших користувачів, перегляд важливих файлів, зміна даних інших користувачів, зміна прав доступу тощо ;

– небезпечна конфігурація оточення (Security Misconfiguration) – неправильна конфігурація окремих компонентів веб – додатків та відсутність оновлень та може нести в собі додаткову загрозу безпеці;

– міжсайтове виконання сценаріїв (XSS) – вразливість, яка з’являється коли web-додаток включає в себе ненадійні дані без належної перевірки, зловмисник отримує можливість виконувати сценарії у браузері жертви, перехоплювати сценарії користувача, перенаправляти користувачів на інші веб - сайти;

– незахищений процес десеріалізації (Insecure Deserialization) – зловмисник може руйнувати логіку роботи веб – додатка, підробляючи об’єкти додатка, що призводить до віддаленого виконання коду зловмисника.

– використання компонентів з відомими вразливостями (Using Components with Known Vulnerabilities) – програмне забезпечення, у якого термін підтримки є неоновленим, може залучити більше зловмисників до його зламу;

– недостатній моніторинг та ведення журналів подій (Insufficient Logging and Monitoring) – погано організований механізм ведення журналів подій та моніторингу може призвести до того, що зловмисники можуть неодноразово робити атаки на веб – додатки, залишаючись непоміченими.

Інший варіант класифікації вразливостей надає Консорціум з безпеки веб - додатків WASC (Web Application Security Consortium).

WASC – це некомерційна організація, яка складається з міжнародної групи експертів, фахівців з інформаційної безпеки, яка послідовно випускає технічну інформацію, статті правила безпеки та інші корисні документи[9].

Згідно документа WASC Threat Classification, вразливості веб – додатків поділяються на наступні етапи життєвого циклу програмного забезпечення[10]:

– етап проектування – вразливості, що можуть з’являтися внаслідок помилок у проектуванні веб – додатка;

– етап реалізації – вразливості, що можуть з’являтися через помилки під час реалізації компонентів веб – додатка.

– етап розгортання – вразливості, що можуть виникати під час налаштування веб – додатка до роботи.

Класифікація вразливостей за етапами життєвого циклу веб – додатка вказана в таблиці 1.1 [10, с. 15].

Таблиця 1.1 – Класифікація вразливостей згідно з WASC Threat Classification за етапами життєвого циклу веб – додатка

| Вразливість | Етапи життевого циклу веб-додатка | | |
|---|---|---|---|
| | Проектування | Реалізація | Розгортання |
| 1 | 2 | 3 | 4 |
| Зловживання функціональністю (Abuse of Functionality) | + | - | - |
| Неправильна конфігурація додатка (Application Misconfiguration) | - | + | - |
| Метод грубої сили (Brute Force) | + | + | - |
| Переповнення буфера (Buffer Overflow) | - | + | - |
| Підміна вмісту (Content Spoofing) | - | + | - |
| Передбачуване значення ідентифікатора сесії (Credential/Session Prediction) | - | + | - |
| Міжсайтовий скриптинг (Cross-Site Scripting) | - | + | - |
| Міжсайтова підробка запиту (Cross-Site Request Forgery) | + | + | - |
| Відмова в обслуговуванні (Denial of Service) | + | + | - |

Продовження табл.1.1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Індексування директорій (Directory Indexing) | - | - | + |
| Атака на функції форматування строк (Format String) | - | - | + |
| Підміна HTTP – відповідей (HTTP Response Smuggling) | - | + | - |
| Розщеплення HTTP – відповідей (HTTP Response Splitting) | - | + | - |
| Підміна HTTP – запитів (HTTP Request Smuggling) | - | + | - |
| Розщеплення HTTP – запитів (HTTP Request Splitting) | - | + | - |
| Переповнення цілого значення (Integer Overflows) | - | + | - |
| Неправильні доступи до файлової системи (Improper Filesystem Permissions) | - | + | + |
| Неправильна обробка вхідних даних (Improper Input Handling) | - | + | - |

Продовження табл.1.1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Неправильна обробка вихідних даних (Improper Output Handling) | - | + | - |
| Витік інформації (Information Leakage) | + | + | + |
| Незахищене індексування (Insecure Indexing) | - | + | + |
| Недостатня протидія автоматизації (Insufficient Anti-automation) | + | + | - |
| Недостатня автентифікація (Insufficient Authentication) | + | + | - |
| Недостатня авторизація (Insufficient Authorization) | + | + | - |
| Недостатнє відновлення пароля (Insufficient Password Recovery) | + | + | - |
| Недостатня перевірка процесу (Insufficient Process Validation) | + | + | - |
| Недостатня тривалість сеансу (Insufficient Session Expiration) | + | + | + |
| Недостатній захист транспортного рівня (Insufficient Transport Layer Protection) | + | + | + |

Продовження табл.1.1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| LDAP ін’єкції (LDAP Injection) | - | + | - |
| Ін’єкції через поштові команди (Mail Command Injection) | - | + | - |
| Ін’єкція нульового байту (Null Byte Injection) | - | + | - |
| Виконання команд ОС (OS Commanding) | - | + | - |
| Зворотній шлях у директоріях (Path Traversal) | - | + | - |
| Прогнозоване місце розташування ресурсів (Predictable Resource Location) | - | + | + |
| Включення віддаленого файлу (Remote File Inclusion (RFI)) | - | + | + |
| Обхідний маршрут (Routing Detour) | - | - | + |
| Неправильна конфігурація сервера (Server Misconfiguration) | - | - | + |
| Фіксація сесії (Session Fixation) | - | + | + |
| SQL ін'єкція | - | + | - |

Продовження табл.1.1

| 1 | 2 | 3 | 4 |
|---|---|---|---|
| Зловживання перенправленням URL (URL Redirector Abuse) | + | + | - |
| XPath ін’єкція (XPath Injection) | - | + | - |
| Переповнення атрибутів XML (XML Attribute Blowup) | - | + | - |
| Аналіз XML – вводу (XML External Entities) | - | + | - |
| Розширення об'єкта XML (XML Entity Expansion) | - | + | - |
| XML ін'єкція (XML Injection) | - | + | - |
| XQuery ін'єкція (XQuery Injection) | - | + | - |

Захищеність веб-додатків залежить від компонентів та технологій, що використовуються при побудові веб-додатків, а також від вразливостей, що можуть виникати у цих компонентах. Причина виникнення вразливостей – помилки при проектуванні, реалізації та застосуванні компонентів веб – додатків. Більшість вразливостей можна виявити задовго до атаки, аналіз вихідного коду веб-додатків дозволяє виявити в кілька разів більше критично небезпечних вразливостей, ніж тестування систем без дослідження коду.

## 1.4 Аналіз популярних CMS

У наш час для найбільш зручного та простого управління вмістом (контентом) часто використовують системи управління вмістом сайту – Content Management System (CMS). Такі системи допомагають веб-майстрам спростити програмування, дизайн, підтримку сайту і навіть поручати роботу з сайтом людям, які не знайомі з програмуванням та архітектурою web.

Система керування вмістом (Content Management System, CMS) — програмне забезпечення для організації веб-сайтів чи інших інформаційних ресурсів в Інтернеті чи окремих комп'ютерних мережах[11]. Код CMS виконується великою частиною на сервері і забезпечує публікацію матеріалів на сайті, а також зручне управління цими публікаціями із веб-інтерфейсу. Безумовно, система керування вмістом має безпосередній вплив на захист веб-додатку.

Основні функції системи керування вмістом [12]:

– надання інструментів для створення вмісту, організація спільної роботи над вмістом;

– управління вмістом: зберігання, контроль версій, дотримання режиму доступу, управління потоком документів і т. п.;

– публікація вмісту;

– подання інформації у виді, зручному для навігації, пошуку.

В залежності від способу розповсюдження розрізняють CMS двох видів: комерційні та вільно поширювані[11].

Безкоштовні CMS поширюються у вільному доступі. Більшість поширених безкоштовних CMS надають безкоштовну підтримку за допомогою спільноти на власних форумах або ж спеціалізованих email-розсилок (наприклад Joomla, WordPress та Drupal).

Платні CMS поділяються на два типи:

– системи із закритим кодом (вихідний код закодований (криптованний) і не допускає будь-яких змін);

– системи з відкритим кодом (для внесення зміни будь-якої з функціональних можливостей вихідний код відкритий).

Згідно з даними сервісу SiteSecure і проекту Ruward[13], які провели комплексне дослідження безпеки сайтів, створених на різних CMS-системах в жовтні 2013 – січні 2014 року, сайти, які користуються безкоштовними CMS, в середньому у 4 рази частіше піддаються зараженням і попадають у чорні списки, ніж сайти на комерційних CMS.

Відповідно даним джерела, частка заражених сайтів представлена на рисунку 1.3


Рисунок 1.3 – Частка заражених сайтів

Згідно з проміжних даних сервісу IT рейтинг України[14] за 2018 рік найпопулярнішими CMS в Україні є:

– WordPress (безкоштовна);
– OpenCart (безкоштовна);
– Joomla (безкоштовна);
– MODX (безкоштовна);
– 1C-Bitrix (платна).

Оскільки система «Бітрікс: Управління сайтом» є найпопулярнішою з комерційних CMS в Україні, є підстави для її перевірки.

## 1.5 Огляд системи «Бітрікс: Управління сайтом» версії 18.x

«Бітрікс: Управління сайтом» — професійна система управління веб-проектами, універсальний програмний продукт для створення, підтримки та успішного розвитку:

– інтернет-магазинів;
– корпоративних сайтів;
– інформаційних порталів;
– сайтів спільнот;
– соціальних мереж та інших веб-проектів.

До складу програмного продукту входить більш ніж 40 модулів для управління інформаційним наповненням та структурою сайту, продажами через інтернет, медіафайлами та фотогалереями, рекламою та багатьма іншими можливостями сайту[15].

Програмний продукт «Бітрікс: Управління сайтом» включає шість редакцій, що розрізняються по функціональними можливостями: від управління контентом сайту до створення портальних інтернет-рішень для електронної торгівлі[16]:

– перший сайт;

– старт;
– стандарт;
– експерт;
– малий бізнес;
– бізнес.

Починаючи з редакції «Стандарт» є можливість користуватися модулем «Проактивний захист», який реалізує основні механізми захисту.

## 1.6 Огляд модуля «Проактивний захист»

Проактивний захист - це комплекс технічних і організаційних заходів, які об'єднані спільною концепцією безпеки і дозволяють значно розширити поняття захищеності та реакції веб-застосунків на загрози[17].

До його складу входять:

– захист від DDoS;
– панель безпеки з рівнями захищеності ;
– проактивний фільтр (Web Application FireWall);
– інструмент для аудиту безпеки PHP-коду;
– веб-антивірус;
– технологія одноразових паролів (OTP);
– генератор одноразових паролів (Bitrix OTP);
– захист авторизованих сесій;
– безпечна авторизація без SSL;
– журнал вторгнень;
– захист адміністративних розділів по IP;
– стоп-листи;
– контроль цілісності скрипта.

### 1.6.1 Захист від DDoS

Одна з поширених причин, за яких сайт може перестати працювати, - DDoS-атака (розподілена атака на сайт за допомогою великого числа «сміттєвих» запитів). Джерела атак та їх технічні реалізації можуть бути різноманітними. Компанії «Бітрікс» і Qrator забезпечують безперервність роботи веб-додатка[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту від DDoS повинна виконуватися функціональна послуга ДС – стійкість до відмов[18].

### 1.6.2 Панель безпеки з рівнями захищеності

За допомогою модуля «Проактивний захист» підвищується захищеність сайту. Для підвищення обирається і налаштовується один з рівнів безпеки модуля: стандартний; високий; підвищений. Система видає рекомендації - яку дію необхідно встановити для кожного параметра на обраному поточному рівні:

– початковий рівень безпеки - отримують проекти на базі Bitrix Framework без встановленого модуля «Проактивний захист»;

– стандартний рівень – у проекті задіяні стандартні інструменти проактивного захисту продукту:

1) проактивний фільтр;
2) журнал вторгнень за останні 7 днів;
3) включений контроль активності;
4) підвищений рівень безпеки для групи адміністраторів;
5) використання CAPTCHA при реєстрації;
6) режим виводу помилок (тільки помилки).

– високий рівень – рекомендований рівень захисту отримують проекти, які виконали вимоги стандартного рівня, і додатково включили:

1) журналювання подій головного модуля;

2) захист адміністративної частини;

3) зберігання сесій в базі даних;

4) зміна ідентифікатора сесій.

– підвищений рівень – спеціальні засоби захисту, обов'язкові для сайтів, що містять конфіденційну інформацію користувачів, для інтернет-магазинів, для тих, хто працює з критичною інформацією. Додатково до високого рівня:

1) включення одноразових паролів;

2) контроль цілісності скрипту контролю[17].

### 1.6.3 Проактивний фільтр (Web Application FireWall)

Проактивний фільтр (WAF - Web Application Firewal) забезпечує захист від більшості відомих атак на веб-додатки. У потоці зовнішніх запитів користувачів проактивний фільтр розпізнає більшість небезпечних загроз і блокує вторгнення на сайт. Проактивний фільтр - найбільш ефективний спосіб захисту від можливих помилок безпеки, допущених при реалізації інтернет-проекту (XSS, SQL Injection, PHP Including і ряду інших). Дія фільтра заснована на аналізі та фільтрації всіх даних, що надходять від користувачів через змінні та куки.

Проактивний фільтр забезпечує:

– захист від більшості відомих атак на веб-застосунки;

– екранування додатку від найбільш активно використовуваних атак;

– створення списку сторінок-винятків з фільтрації (по масці);

– розпізнавання більшості небезпечних загроз;

– блокування вторгнень на сайт;

– захист від можливих помилок безпеки;

– фіксування спроб атак в журналі;

– інформування адміністратора про випадки вторгнення;

– налаштування активної реакції - дій системи при спробі вторгнення на сайт:

1) зробити дані безпечними;

2) очистити небезпечні дані;

3) додати IP адреса атакуючого в стоп-лист на XX хвилин;

4) занести спробу вторгнення в журнал.

– оновлення разом з продуктом[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою проактивного фільтра повинні виконуватися такі функціональні послуги: НР – реєстрація, НИ – ідентифікація і автентифікація[18].

### 1.6.4 Інструмент для аудиту безпеки PHP-коду

Інструмент для аудиту безпеки PHP-коду - інструмент для розробника, який «підказує» вузькі місця в безпеці його коду. Інструмент дозволяє не тільки запобігти експлуатацію вразливості, але й усунути її джерело. Перевірка показує в звіті потенційно вразливі місця в коді та підсилює захист сайту від злому[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою аудиту безпеки PHP-коду повинні виконуватися такі функціональні послуги:, [18].

### 1.6.5 Веб-антивірус

«Веб-антивірус» перешкоджає імплантуванню шкідливого коду безпосередньо в веб-додатки. Він виявляє в HTML коді потенційно небезпечні ділянки і «вирізає» підозрілі об'єкти з коду сайту. У підсумку віруси не можуть потрапити до електронної пошти користувача сайту - антивірус перешкоджає цьому. «Веб-антивірус» повідомляє адміністратора порталу - попереджає про наявність вірусу. Отримуючи інформацію про це, адміністратор шукає джерело шкідливого коду, проводить «зачистку» комп'ютера і підсилює профілактичні заходи[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою аудиту безпеки PHP-коду повинні виконуватися такі функціональні послуги: НР – реєстрація [18].

### 1.6.6 Технологія одноразових паролів (OTP)

Модуль «Проактивний захист» дозволяє включити підтримку одноразових паролів і використовувати їх вибірково для будь-яких користувачів на сайті. Рекомендується задіяти систему одноразових паролів адміністраторам сайтів, оскільки це сильно підвищує рівень безпеки користувальницької групи «Адміністратори».

Система одноразових паролів доповнює стандартну систему авторизації та дозволяє значно посилити систему безпеки інтернет-проекту. Для включення системи необхідно використовувати апаратний пристрій (наприклад, Aladdin eToken PASS або відповідне програмне забезпечення, що реалізує OTP).

Одноразовий пароль (OTP) — це пароль, який є дійсним тільки для одного сеансу автентифікації. Його дія також може бути обмежена певним проміжком часу. Перевага такого паролю порівняно зі статичним полягає в тому, що його неможливо використовувати повторно. Таким чином, зловмисник, що перехопив дані з успішної сесії автентифікації, не може використовувати скопійований пароль для отримання доступу до захищеної інформаційної системи[19].

Це метод захисту від шпигунських програм за допомогою авторизації в два етапи. Перший - це основний логін і пароль користувача. Другий - це одноразовий код, який кожен користувач отримує з програми в своєму мобільному телефоні або зі спеціального пристрою. В результаті, навіть якщо логін і пароль будуть вкрадені, зловмисники не зможуть ними скористатися без одноразового коду.

Система авторизації з використанням одноразових паролів (One-Time Password - OTP) розроблена в рамках ініціативи OATH.

Реалізація заснована на алгоритмі HMAC і хеш-функцій SHA-1 / SHA-256 / SHA-512. На поточний момент підтримується два алгоритму генерації:

– за лічильником (HMAC-Based One-time Password, HOTP);

– за часом (Time-based One-time Password, TOTP).

Для розрахунку значення OTP приймаються два вхідних параметра - секретний ключ (початкове значення для генератора) і поточне значення лічильника (кількість необхідних циклів генерації або поточний час, в залежності від обраного алгоритму). Початкове значення зберігається як в самому пристрої, так і на сайті після його запуску. У разі використання HOTP алгоритму, лічильник в пристрої збільшується при кожній генерації OTP, на сервері - при кожному вдалому аутентифікації по OTP. У разі використання TOTP алгоритму, лічильник в пристрої не зберігається, на сервері лише коригується можливе невелике зміщення часу пристрою при кожному вдалому аутентифікації по OTP.

Партія пристроїв OTP поставляється з зашифрованим файлом, що містить початкові значення (секретні ключі) для всіх пристроїв партії, пов'язаного з серійним номером пристрою (друкується на корпусі пристрою).

У разі порушення синхронізації лічильника генерації в пристрої і на сервері, її можна легко відновити - привести значення на сервері у відповідність значенням, що зберігається в пристрої. Для цього адміністратор системи або сам користувач (при наявності відповідних дозволів) повинен згенерувати два послідовних значення одноразових паролів (OTP) і ввести їх в форму на сайті. Мобільний додаток для генерації одноразового пароля є в GooglePlay і AppStore[20].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою технології одноразових паролів (OTP) повинні виконуватися такі функціональні послуги: НИ – ідентифікація і автентифікація, НК – достовірний канал[18].

### 1.6.7 Генератор одноразових паролів (Bitrix OTP)

За допомогою Bitrix OTP є можливість самостійно включати або відключати використання на сайті системи одноразових паролів для облікових записів. Це реалізує OTP програмне забезпечення, розроблене компанією «Бітрікс24», дозволяє обійтися без покупки апаратних пристроїв (наприклад, Aladdin eToken PASS) або відповідних програмних аналогів.

Є можливість включити на мобільному сайті підтримку одноразових паролів і використовувати їх вибірково для будь-яких користувачів. Особливо рекомендується задіяти систему одноразових паролів адміністраторам сайтів, оскільки це сильно підвищує рівень безпеки для користувача групи «Адміністратори». Для цього достатньо створити в генераторі паролів новий сайт, який підтримує авторизацію по OTP, і потім кожен раз, при вході на цей сайт, отримувати для нього одноразовий пароль. Генератор дозволяє створити безліч записів для таких сайтів, і потрібний сайт ви зможете вибрати зі списку[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою використання генератора одноразових паролів (OTP) повинні виконуватися такі функціональні послуги: НИ – ідентифікація і автентифікація, НК – достовірний канал[18].

### 1.6.8 Захист авторизованих сесій

Більшість атак на веб-додатки ставлять метою отримати дані про авторизованої сесії користувача. Включення захисту сесій робить викрадення авторизованої сесії неефективним. І, якщо мова йде про авторизованої сесії адміністратора, то її надійний захист за допомогою даного механізму є особливо важливим завданням.

Зберігання даних сесій в таблиці модуля дозволяє уникнути читання цих даних через скрипти інших сайтів на тому ж сервері, виключивши помилки

конфігурування віртуального хостингу, помилки налаштування прав доступу у тимчасових каталогах і ряд інших проблем налаштування операційного середовища. Крім того, це розвантажує файлову систему, переносячи навантаження на сервер бази даних.

Захист сесій забезпечує:

– захист кількома способами:

1) час сесії життя (хвилини);

2) зміна ідентифікатора сесії раз на кілька хвилин;

3) маска мережі для прив'язки сесії до IP;

4) зберігання даних сесій в таблиці модуля.

– виключення помилок конфігурування віртуального хостингу;

– виключення помилок налаштування прав доступу у тимчасових каталогах;

– виключення проблем налаштування операційної середовища;

– розвантаження файлової системи;

– марність викрадення сесій зловмисниками[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою захисту авторизованих сесій повинні виконуватися такі функціональні послуги: НИ – ідентифікація і автентифікація[18].

### 1.6.9 Безпечна авторизація без SSL

За допомогою методики безпечної автентифікації паролі з форми авторизації співробітників неможливо зламати, оскільки вони шифруються за алгоритмом RSA з ключем 1024 біт і в такому вигляді передаються на корпоративний портал. При цьому не важливо, які з'єднання і протоколи використовують користувачі порталу.

Переваги використання:

– безпечна автентифікація шифрування пароля дозволяє уникнути передачі пароля у відкритому вигляді без SSL;

– всі інструменти, які використовувалися раніше для авторизації, продовжать працювати[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою безпечної авторизації без SSL повинні виконуватися такі функціональні послуги: КВ – конфіденційність при обміні[18].

### 1.6.10 Журнал вторгнень

У журналі реєструються події, що відбуваються в системі, в тому числі незвичайні або зловмисні. Оперативний режим реєстрації цих подій дозволяє переглядати відповідні записи в журналі відразу ж після їхньої генерації. У свою чергу, це дозволяє виявляти атаки і спроби атак в момент їх проведення. Це значить, що є можливість негайно приймати відповідні заходи, і, в деяких випадках, навіть попереджати атаки.

Переваги використання:

– оперативна реєстрація всіх подій в системі;

– у разі спрацювання Проактивного фільтра запис у журналі в одній з категорій атак:

1) спроба впровадження SQL;
2) спроба атаки через XSS;
3) спроба впровадження PHP.

– відбір зловмисних подій по фільтру;

– перегляд та аналіз подій в реальному часі;

– негайна реакція - відповідна міра на подію;

– профілактика і попередження подій на основі їх аналізу[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою журналу вторгнень повинні виконуватися такі функціональні послуги: НР – реєстрація[18].

### 1.6.11 Захист адміністративних розділів по IP

Цей захист дозволяє компаніям строго регламентувати мережі, які вважаються безпечними і з яких дозволяється працівникам адмініструвати сайт. Це простий спеціальний інтерфейс, в якому все це і робиться - задається список або діапазони IP-адрес, з яких дозволяється управління сайтом. Закривання доступу у момент встановлення блокування перевіряється системою.

Ефект від використання даного захисту полягає в тому, що будь-які XSS/CSS атаки на комп'ютер користувача стають неефективними, а викрадення перехоплених даних для авторизації з чужого комп'ютера - марними.

Переваги використання:

– обмеження доступу до адміністративної частини всіх IP-адрес, крім зазначених;

– автоматичне визначення системою IP адреси користувача;

– ручне введення дозволеної IP адреси;

– установка діапазону IP-адрес, з яких дозволений доступ до адміністративної частини[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою журналу вторгнень повинні виконуватися такі функціональні послуги: НК – достовірний канал[18].

### 1.6.12 Стоп-листи

Стоп-лист – це таблиця, яка містить параметри, які використовуються для обмеження доступу відвідувачів до вмісту сайту і перенаправлення на інші сторінки. Всі користувачі, які спробують зайти на сайт з IP адресами, включеними в стоп-лист, будуть заблоковані.

Переваги використання:

– перенаправлення відвідувачів, параметри яких містяться в стоп-листі;

– блокування користувачів по IP адресам із стоп-листа;

– ручне поповнення стоп-листа новими записами;

– облік статистики користувачів, яким заборонено доступ до сайту;

– встановлення періоду дії заборони на доступ до сайту для користувача, IP-мережі, маску мережі, UserAgent і посилання, за яким прийшов користувач;

– змінюване повідомлення, яке буде показано користувачу при спробі доступу до сайту[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою стоп-листів повинні виконуватися такі функціональні послуги: НИ – ідентифікація і автентифікація обов’язків[18].

### 1.6.13 Контроль цілісності скрипта

Контроль цілісності файлів необхідний для швидкого з'ясування - чи вносилися зміни в файли системи. У будь-який момент ви можете перевірити цілісність ядра, системних областей, публічної частини продукту.

Перед перевіркою цілісності системи є необхідність перевіряти скрипт контролю на наявність змін. При першому запуску скрипта вводиться довільний пароль (що складається з латинських букв і цифр, довжиною не менше 10 символів), а також довільне кодове (ключове слово (відмінне від пароля), і натискається кнопка «Встановити новий ключ».

Переваги використання:

– перевірка скрипта на наявність змін;

– захист цілісності скрипта ключем - символьним паролем[17].

Відповідно до НД ТЗІ 2.5-004-99 для забезпечення захисту за допомогою контролю цілісності скрипта повинні виконуватися такі функціональні послуги: НТ – самотестування[18].

## 1.7 Висновки до першого розділу

Проблема безкоштовних CMS в тому, що при розширенні функціональності сайту, використовуються спеціальні плагіни, враховуючи їх недостатній рівень безпеки можливі утворення вразливостей. Крім того, системи постійно удосконалюються, і їх необхідно своєчасно оновлювати. Тому зломи сайтів на безкоштовних CMS найчастіше відбуваються через ігнорування нових версій систем і після установлення плагінів сумнівного походження.

Платні CMS при дослідженні кількості злому сайтів на різних CMS виявляються більш безпечними, при використанні платних систем складніше пропустити важливі оновлення а значить, підвищуються шанси підвищити базовий рівень безпеки.

Оскільки система «Бітрікс: Управління сайтом» виходячи з даних сервісу IT рейтинг України[14] є найпопулярнішою комерційною CMS в Україні, комплекс засобів захисту захищеного програмного комплексу «1С-Битрикс: Управління сайтом» версії 15.х входить до переліку засобів ТЗІ дозволених для забезпечення технічного захисту державних інформаційних ресурсів, але експертний висновок не є на разі дійсним[21], і враховуючи, що версія продукту оновилася до 18, що призвело до певних змін (наприклад, з’явилася сумістність з PHP 7) є підстави для перевірки ефективності елементів модуля «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х. На сьогоднішіній день актуальною є версія 18.1.3.

При створенні систем захисту згідно з вимогами НД ТЗІ 3.7-003-05[22] у випадку використання засобів захисту які на момент проектування КСЗІ не мали відповідного сертифікату або експертного висновку необхідно передбачити оцінку цих засобів на відповідність НД ТЗІ. Крім того таку оцінку необхідно проводити під час державної експертизи.

# РОЗДІЛ 2. ПЕРЕВІРКА ЕЛЕМЕНТІВ МОДУЛЯ «ПРОАКТИВНИЙ ЗАХИСТ» СИСТЕМИ «БІТРІКС: УПРАВЛІННЯ САЙТОМ» ВЕРСІЇ 18.X

Оскільки в історії версій модуля «Проактивний захист»[23], у березні 2016 року у версії 16.0.2 «Бітрікс: Управління сайтом» було впроваджено сумістність з PHP 7, у версії 17.0.0 було виправлене зберігання сесій у базі даних у PHP 7 , а у версії 17.0.1 покращена сумістність з PHP 7, є доцільною перевірка елементів цього модулю.

Оскільки впровадження PHP 7 є важливим фактором для веб-додатків, є доцільним розглянути версію більш детально.

3 грудня 2015 року було оголошено про вихід PHP версії 7.0.0. Нова версія грунтується на експериментальній гілці PHP, яка спочатку називалася phpng (PHP Next Generation - наступне покоління), і розроблялася з упором на збільшення продуктивності і зменшення споживання пам'яті. У новій версії додана можливість вказувати тип даних з функції, що повертаються, доданий контроль переданих типів для скалярних даних, а також нові оператори[24].

По даним декількох декількох джерел[25][26] за допомогою php 7 швидкість роботи сайту збільшується приблизно у 2 рази порівняно з попередньою версією.

Рівнем гарантій послуг приймається рівень Г-2, але в даній роботі не розглядається, оскільки критерії гарантій включають вимоги до архітектури комплексу засобів захисту, середовища розробки, послідовності розробки, випробування комплексу засобів захисту, середовища функціонування і експлуатаційної документації.

## 2.1 Формулювання завдання

Для перевірки елементів модуля «Проактивний захист» системи «Бітрікс: Управління сайтом» вирішено керуватися нормативними документами НД ТЗІ 2.5-004-99 та НД ТЗІ 2.7-009-09.

Згідно з НД ТЗІ 2.5-004-99 «В процесі оцінки спроможності комп'ютерної системи забезпечувати захист оброблюваної інформації від несанкціонованого доступу розглядаються вимоги двох видів:

– вимоги до функцій захисту (послуг безпеки);

– вимоги до гарантій.

В контексті Критеріїв комп'ютерна система розглядається як набір функціональних послуг. Кожна послуга являє собою набір функцій, що дозволяють протистояти певній множині загроз. Кожна послуга може включати декілька рівнів. Чим вище рівень послуги, тим більш повно забезпечується захист від певного виду загроз. Рівні послуг мають ієрархію за повнотою захисту, проте не обов'язково являють собою точну підмножину один одного. Рівні починаються з першого (1) і зростають до значення n, де n — унікальне для кожного виду послуг»[18].

## 2.2 Загальні положення щодо проведення програми і методики послуг безпеки

Випробування системи «Бітрікс: Управління сайтом» проводяться на підставі керівних документів:

– НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу[5];

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу[18];

– НД ТЗІ 2.7 -009-09. Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу[27].

При виконанні роботи, будуть перевірятися наступні функціональні послуги безпеки:

– НК – достовірний канал;

– НИ – ідентифікація і автентифікація;

– НО – розподіл обов'язків;

– НР – реєстрація;

– КВ – конфіденційність при обміні;

– НЦ – цілісність КЗЗ;

– НТ – самотестування.

2.3 Програма і методика випробувань функціональної послуги безпеки «Достовірний канал» рівня НК-1 – «Однонаправлений достовірний канал»

2.3.1 Програма випробувань

– Перевірка механізмів встановлення достовірного зв’язку між користувачем та КЗЗ.

– Перевірка того, що достовірний канал використовується для початкової ідентифікації та автентифікації, зв’язок з використанням цього каналу ініціюється винятково користувачем.

2.3.2 Методика випробувань

– Перевірка механізмів встановлення достовірного зв’язку між користувачем та КЗЗ. Перевірка того, що достовірний канал використовується для початкової ідентифікації та автентифікації, зв’язок з використанням цього каналу ініціюється винятково користувачем.

1) Перевіряється для всіх типів користувачів спроби ініціювання достовірного каналу між користувачем та КЗЗ. Достовірний канал повинен ініціюватися при спробі кожного типу користувача.

2) Перевіряється можливість виконання спроби підміни компонента КЗЗ, з яким ініціюється взаємодія, або доводиться неможливість виконання такої підміни. Виконання спроби підміни компонента КЗЗ повинне бути неможливе.

### 2.3.3 Результати випробування

У системі «Бітрікс: Управління сайтом», на сайті, що перевіряється[28] установлені такі групи користувачів:

– адміністратори;

– усі користувачі (у тому числі не авторизовані);

– зареєстровані користувачі;

– адміністратори інтернет-магазину;

– контент-редактори.

Для забезпечення достовірного каналу між користувачем та КЗЗ підключено технологію одноразових паролів (OTP). Підключення одноразових паролів відбувається  на відповідній сторінці модуля, що показано на рисунку 2.1.

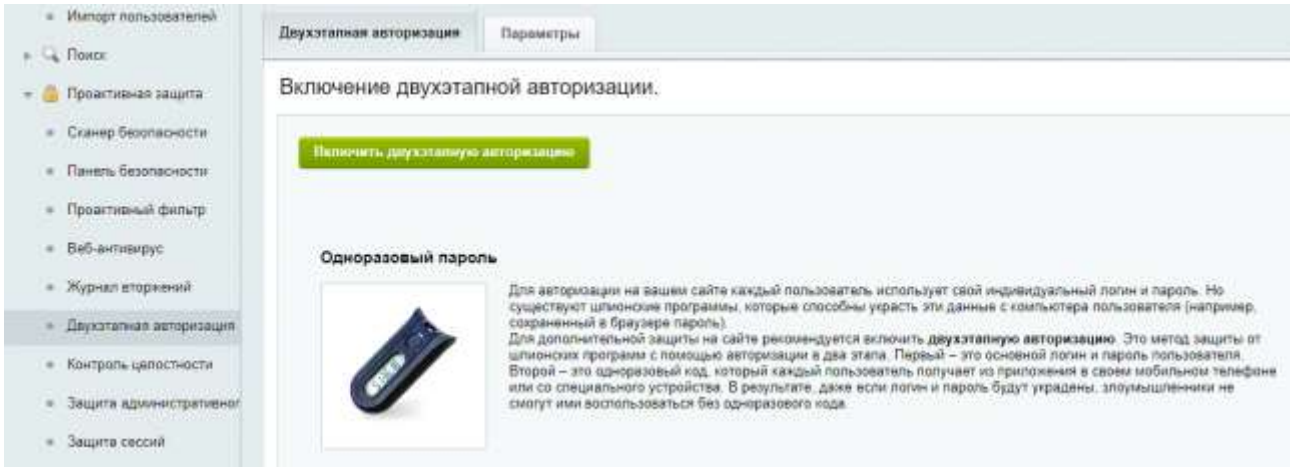



Рисунок 2.1 – Панель включення використання одноразових паролів

Після цього, для кожного типу користувача підключене OTP програмне забезпечення, розроблене компанією «Бітрікс24», що дозволяє обійтися без покупки апаратних пристроїв, що показано на рисунку 2.2.


Рисунок 2.2 – Панель включення програмного забезпечення OTP

Потім за допомогою мобільного додатку (програмного забезпечення OTP) просканово QR-код та введені 2 послідовно згенеровані коди, що показано на рисунку 2.3, що дозволяє підключити використання одноразових паролів.

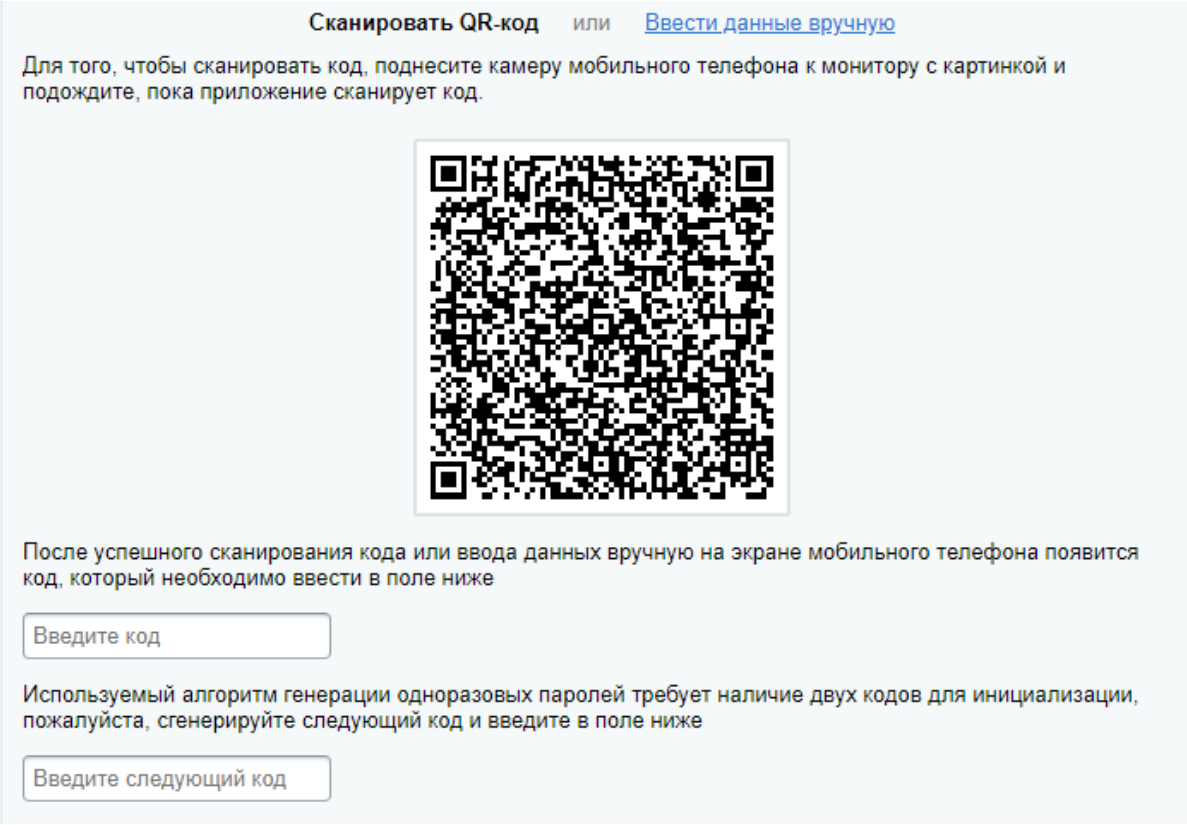



Рисунок 2.3 – Панель налаштування одноразових паролів

Оскільки потрібно встановити початкове значення лічильника успішних процедур автентифікації на веб-сайті, було послідовно згенеровано два пароля і введено їх у відповідні поля форми, що показано на рисунку 2.4. Після цього

пристрій (мобільний додаток) пов'язаний з профайлом користувача та ініціалізований.

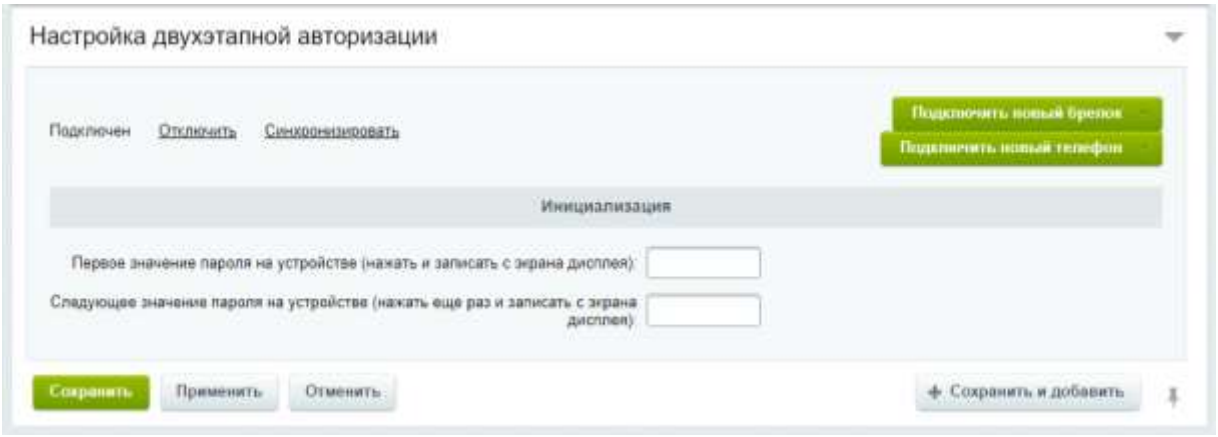



Рисунок 2.4 – Панель встановлення початкового значення лічильника успішних процедур автентифікації на веб-сайті

Було перевірено спроби автентифікації усіма користувачами, для яких встановлено використання одноразових паролів, після вводу логіну та паролю повинен бути введений одноразовий пароль, що показано на рисунку 2.5.

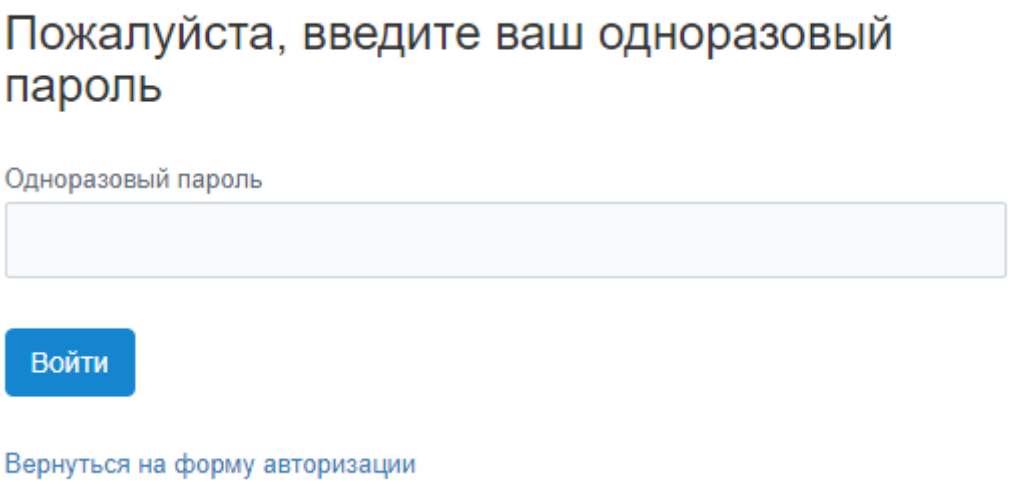



Рисунок 2.5 – Необхідність введення одноразового паролю

При порушенні синхронізації лічильника успішних процедур автентифікації (при багатократній зміні коду у мобільному додатку без воду проля, або багатократних спробах вводу пароля, без зміни коду у мобільному

додатку) у користувача немає можливості увійти на сайт, що показано на рисунку 2.6.

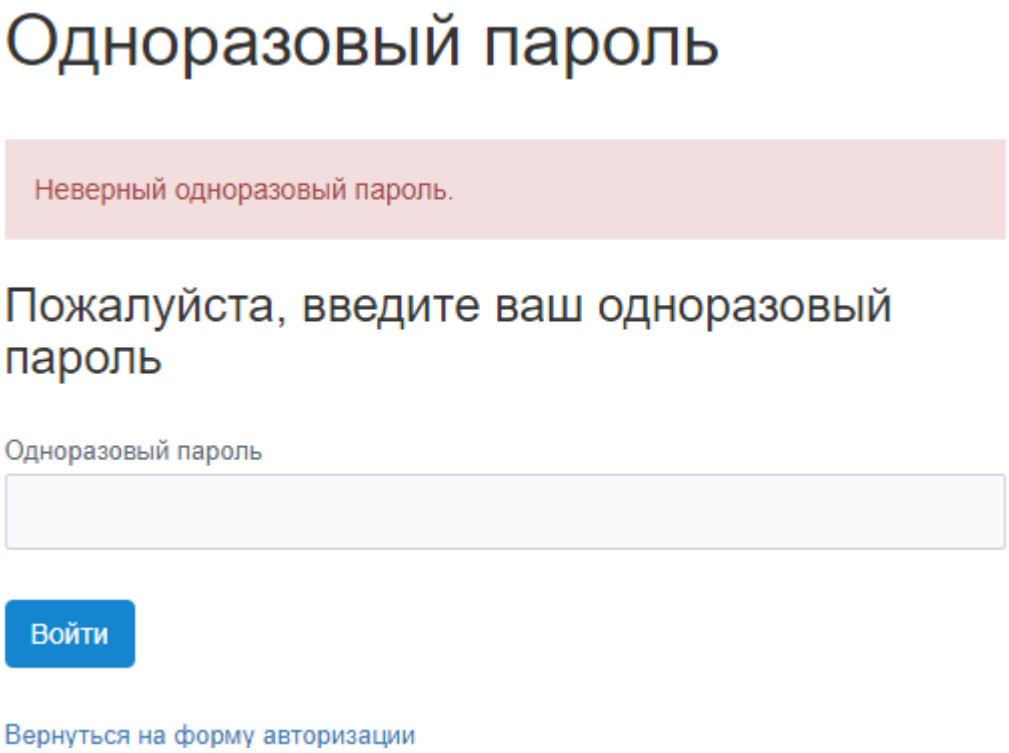



Рисунок 2.6 – Унеможливлення входу при порушенні синхронізації лічильника

Лише після приведення значення лічильника на сервері у відповідність значенням, що зберігається в пристрої, що може зробити адміністратор використання одноразових паролів доступно.

Отже, було перевірено, що кожен користувач може користуватися технологією одноразових паролів. Виконання спроби підміни компонента КЗЗ неможливе, оскільки автентифікаційні дані - це результат шифрування будь-якого початкового значення за допомогою секретного ключа користувача. Дана інформація є і у клієнта, і у сервера. Вона не передається по мережі і недоступна для перехоплення. В якості початкового значення використовується відома обом сторонам процесу автентифікації інформація, а ключ шифрування створюється для кожного користувача при його ініціалізації в системі.

## 2.4 Програма і методика випробувань функціональної послуги безпеки «Ідентифікація та автентифікація» рівня НИ-2 – «Одиночна ідентифікація та автентифікація»

### 2.4.1 Програма випробувань

– Перевірка атрибутів, якими характеризуються користувачі різного типу і перевірка послуг, для використання яких необхідні ці атрибути.

– Перевірка користувачів для кожного типу на однозначність ідентифікації на підставі атрибутів.

– Перевірка на те, що перед тим, як дозволити користувачу будь-якого типу виконувати контрольовані дії КЗЗ ОЕ, система здатна авентифікувати цього користувача.

– Перевірка забезпечення захисту даних автентифікації від несанкціонованого доступу, модифікації або руйнування.

– Перевірка на використання засобів реалізації послуги «Достовірний канал» рівня НК-1 або вище при взаємодії користувача будь-якого типу з КЗЗ ОЕ в процесі автенифікації.

### 2.4.2 Методика випробувань

– Перевірка на використання засобів реалізації послуги «Достовірний канал» рівня НК-1 або вище при взаємодії користувача будь-якого типу з КЗЗ ОЕ в процесі автенифікації.

1) Перевіряється виконання для всіх типів користувачів випробувань засобів реалізації функціональної послуги безпеки «Достовірний канал» рівня НК-1 – «Однонаправлений достовірний канал». Функціональна послуги безпеки «Достовірний канал» рівня НК-1 – «Однонаправлений достовірний канал» повинна виконуватися для всіх типів користувачів.

– Перевірка пунктів 1, 2, 3 програми випробувань.

1) Перевіряються спроби ідентифікації та автентифікації кожного типу користувача. Для кожного типу користувача повинні бути відповідні доступи до виконання функціональних послуг безпеки.

2) Перевіряються можливість виконання функціональних послуг безпеки, для виконання яких потрібні атрибути користувача. Кожна послуга повинна виконуватися для відповідного користувача.

3) Перевіряється можливість виконання спроби несанкціонованого входу з пред'явленням хибних даних авторизації. При спробах несанкіцонованого входу, доступ до інформаційних ресурсів не дозволяється.

– Перевірка забезпечення захисту даних автентифікації від несанкціонованоо доступу, модифікації або руйнування.

1) Перевіряються механізми та порядок захисту даних автенитфікації при спробах несанкціонованого входу, модифікації, або руйнування.

### 2.4.3 Результати випробування

Виконання перевірки функціональної послуги безпеки «Достовірний канал» рівня НК-1 – «Однонаправлений достовірний канал» показана в пункті 2.4.3.

У системі «Бітрікс: Управління сайтом» для кожної групи користувачів є відповідні доступи до функціональних модулів системи. Перевіривши спроби ідентифікації та автентифікації різних типів користувачів, отримано висновки, що при автенитифікації користувача групи "адміністратори" надається повний доступ до модуля «Проактивний захист», що показано на рисунку 2.7.

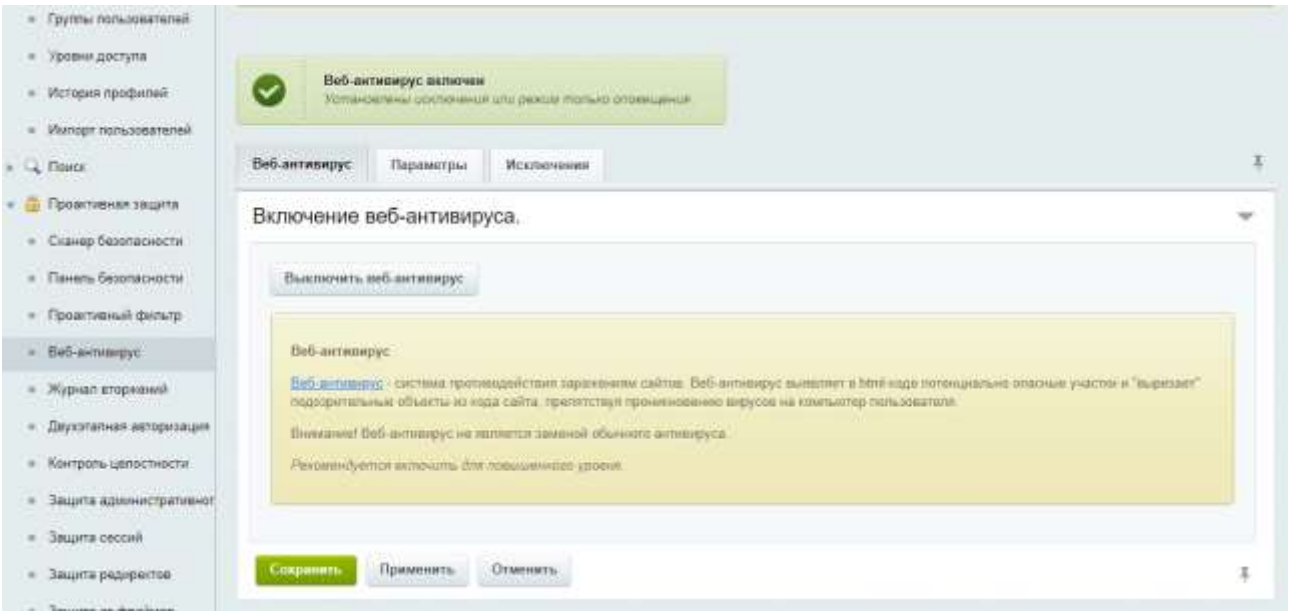



Рисунок 2.7 – Повний доступ до модуля «Проактивний захист»

При автенитифікації користувача групи “адміністратори інтернет-магазину” надається лише частковий доступ до модуля «Проактивний захист», а саме – перегляд даних, що показано на рисунку 2.8. Для усіх інших груп користувачів доступ до модуля закритий.

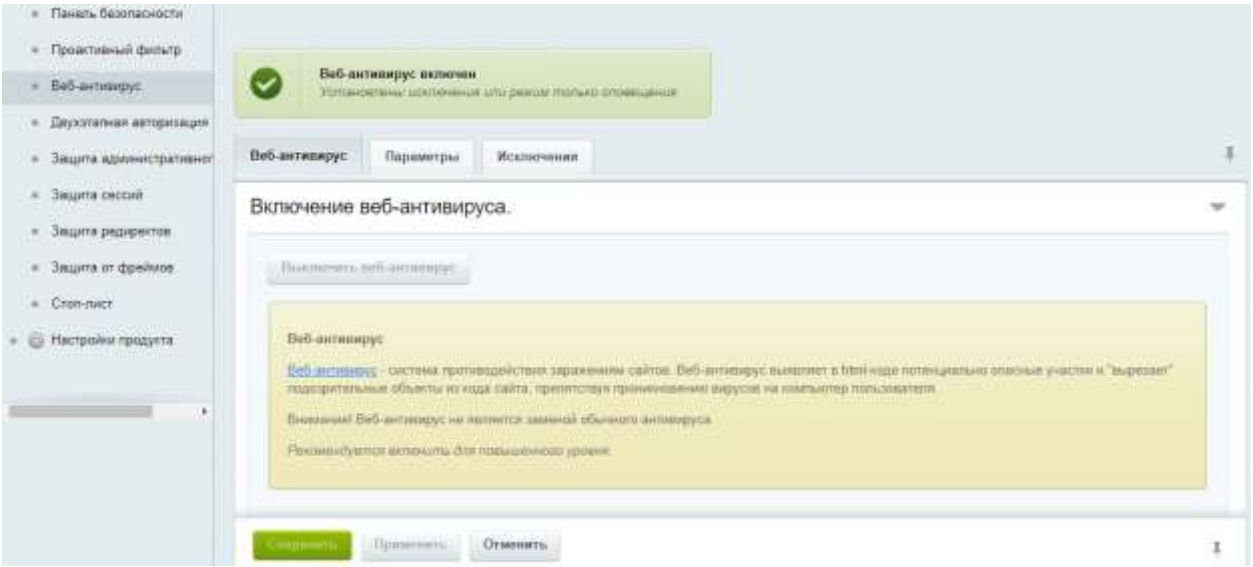



Рисунок 2.8 – Частковий доступ до модуля «Проактивний захист»

Перевірено, що лише користувачі групи “адміністратори” мають доступ до роботи з модулем «Проактивний захист», та мають можливість виконання функціональних послуг безпеки.

Перевірено, що при спробах несанкіцонованого входу з пред’явленням хибних даних авторизації, доступ до інформаційних ресурсів не дозволяється.

Для захисту даних авторизації використовується захист сесій, що виконується за допомогою зберігання даних сесій в таблиці модуля та зміни ідентифікатора сесії через кожні 60 секунд, що показано на рисунках 2.9 та 2.10.

Зберігання даних сесій в таблиці модуля дозволяє уникнути читання цих даних через скрипти інших віртуальних серверів, виключивши помилки конфігурації віртуального хостингу, помилки настройки прав доступу у тимчасових каталогах і ряд інших проблем настройки операційного середовища. Також це розвантажує файлову систему, переносячи навантаження на сервер бази даних.

При включенні зміни ідентифікатора сесії користувача, ідентифікатор змінюється через заданий проміжок часу. Це створює додаткове навантаження на сервер, але дозволяє зробити викрадення авторизованої сесії неефективним.

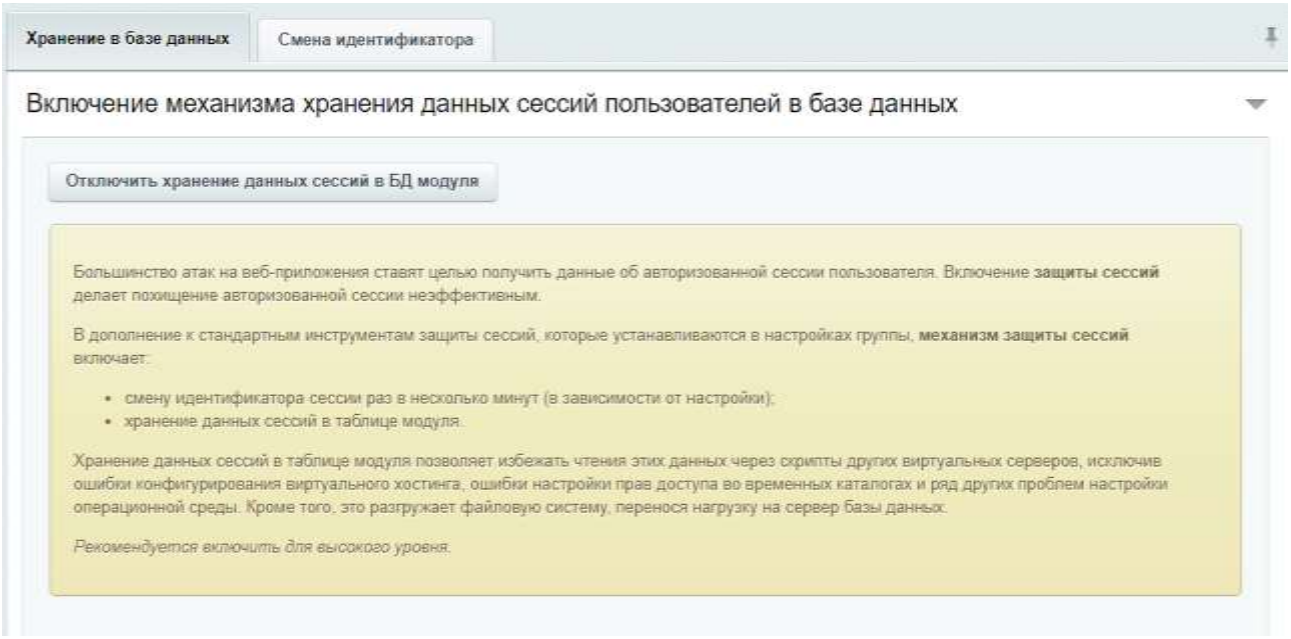



Рисунок 2.9 – Панель підключення механізму зберігання даних сесій користувачів у базі даних

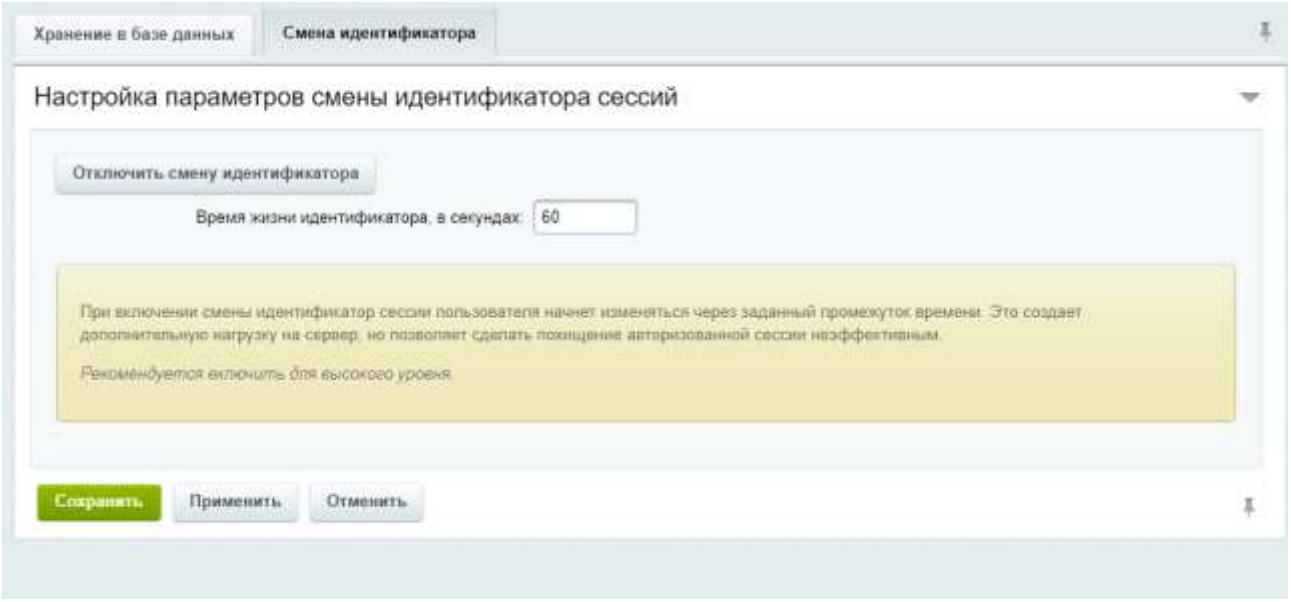



Рисунок 2.10 – Панель зміни ідентифікатора

Додатковими інструментами для забезпечення ідентифікації та автентифікації є використання елементів модуля «Проактивний захист»: «Захист адміністративних розділів по IP» та «Стоп лист». Завдяки захисту адміністративних розділів по IP можна зробити обмеження доступу до адміністративної частини для всіх IP-адрес, крім тих які указуються адміністратором. Завдяки стоп листам виконується обмеження доступу відвідувачів до вмісту сайту і відбувається перенаправлення на інші сторінки. Всі користувачі, які спробують зайти на сайт з IP адресами, включеними в стоп-лист, будуть заблоковані.

## 2.5 Програма і методика випробувань функціональної послуги безпеки «Розмежування обов'язків» рівня НО-1 – «Виділення адміністратора»

### 2.5.1 Програма випробувань

– Перевірка визначення ролі адміністратора та звичайного користувача та притаманні їм функції.

– Перевірка підтримання засобами КЗЗ призначення користувачів на відповідні ролі згідно з атрибутами доступу.

– Перевірка того, що користувачі мають можливість виступати у певній ролі лише після того, як вони виконують певні дії, що підтверджують прийняття ними цієї ролі.

– Перевірка автентифікації рівня НИ-1 або вище атрибутів користувачів, перед виконанням призначення цих користувачів на роль.

### 2.5.2 Методика випробувань

– Перевірка автентифікації рівня НИ-1 або вище атрибутів користувачів, перед виконанням призначення цих користувачів на роль.

1) Перевіряється виконання для користувачів, які відносяться до всіх типів ролей, випробувань засобів реалізації функціональної послуги безпеки «Ідентифікація та автентифікація». Функціональна послуга безпеки «Ідентифікація та автентифікація» повинна бути виконана для користувачів усих типів ролей.

– Перевірка визначення ролі адміністратора та звичайного користувача та притаманні їм функції.

1) Перевіряються та описуються ролі і функції адміністратора та звичайного користувача. Ролі повинні бути чітко визначеними, а функції ролі виконуватися тільки для відповідної ролі.

– Перевірка пунктів 2, 3 програми випробувань.

1) Перевіряється можливість призначення користувачів на відповідні ролі та доступність, чи недоступність їм відповідних функцій. Повинне відбуватися призначення користувача на відповідну роль, а відповідні функції повинні бути доступні.

2) Перевіряється можливість призначення користувачів на відповідні ролі лише у випадку виконанням користувачем дій, що підтверджують прийняття користувачем певної ролі. Після виконання дій що підтверджують користувачів

певної ролі, повинна виконуватися можливість призначення користувача на відповідну роль.

### 2.5.3 Результати випробування

Функції, що належать для кожного типу користувачів, залежать від рівня доступу групи користувача до кожного функціонального модулю, що показано на таблиці 2.1.

Перевірено, що призначення користувача на відповідну роль відбувається, а відповідні функції доступні, що показано на рисунках 2.11 – 2.13.

При присвоєнні користувачу групи «Адміністратор інтернет-магазину» для нього є доступний перегляд модулю «Проактивний захист» без доступу до використання функцій.

Призначення користувачів на відповідні ролі лише у випадку виконанням користувачем дій, що підтверджують прийняття користувачем певної ролі передбачає, що перед присвоєнням ролі, користувачу потрібно заповнити відповідну документацію, для надання йому ролі. Це відноситься до організаційних питань і в даній дипломній роботі не розглядається

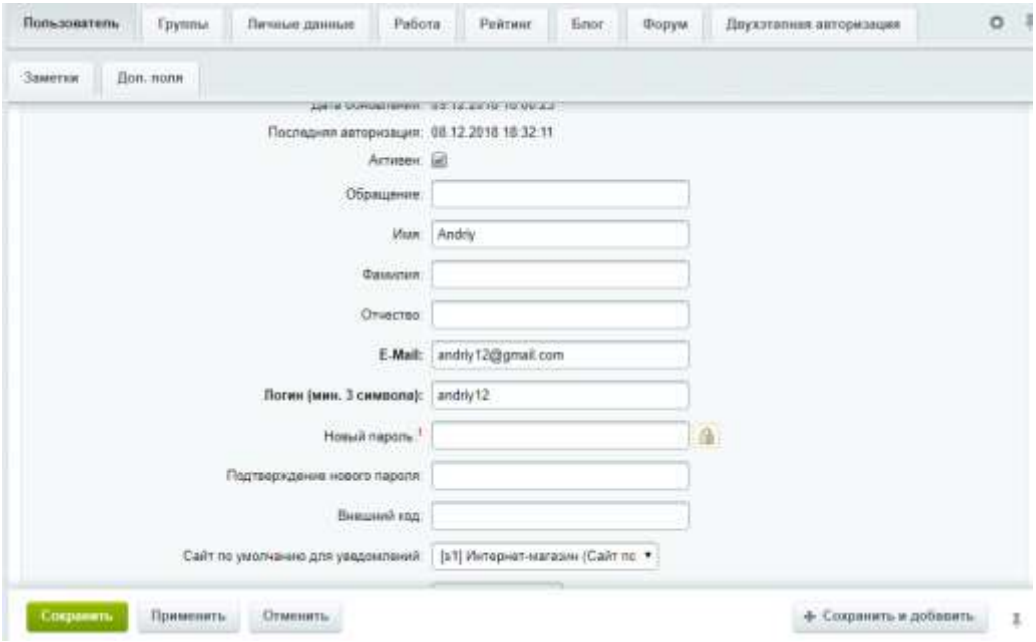



Рисунок 2.11 – Сторінка профілю користувача

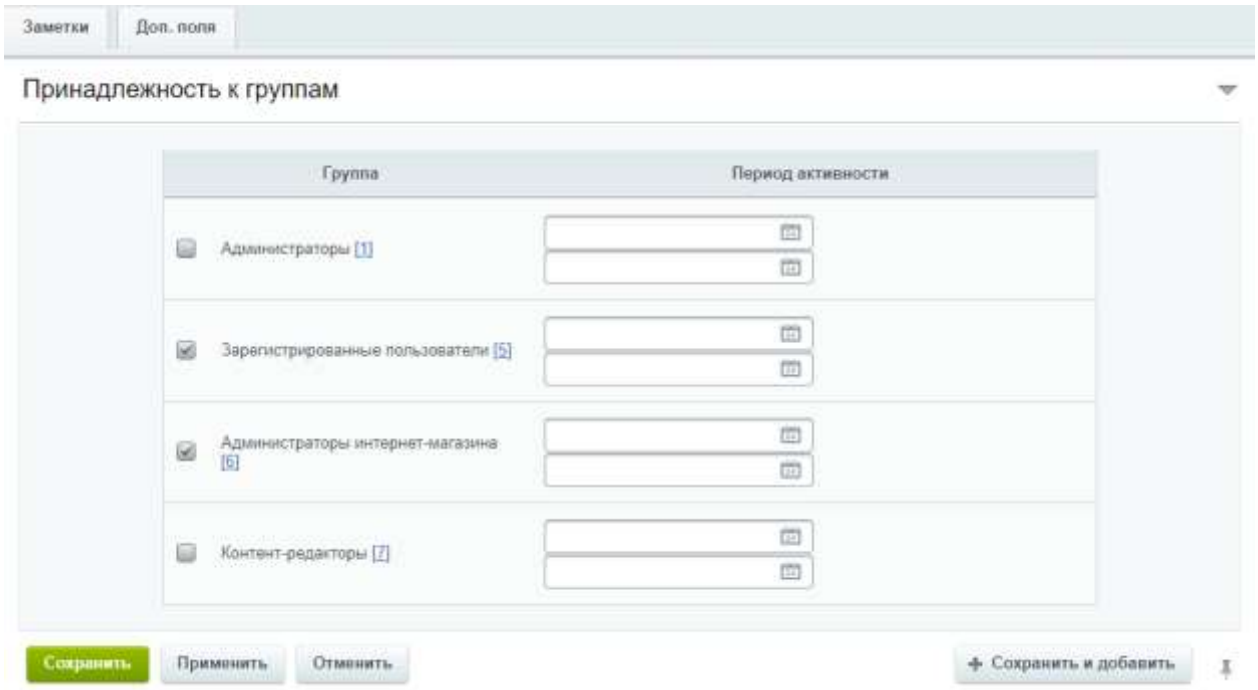



Рисунок 2.12 – Сторінка з інформацією про належность користувача до груп

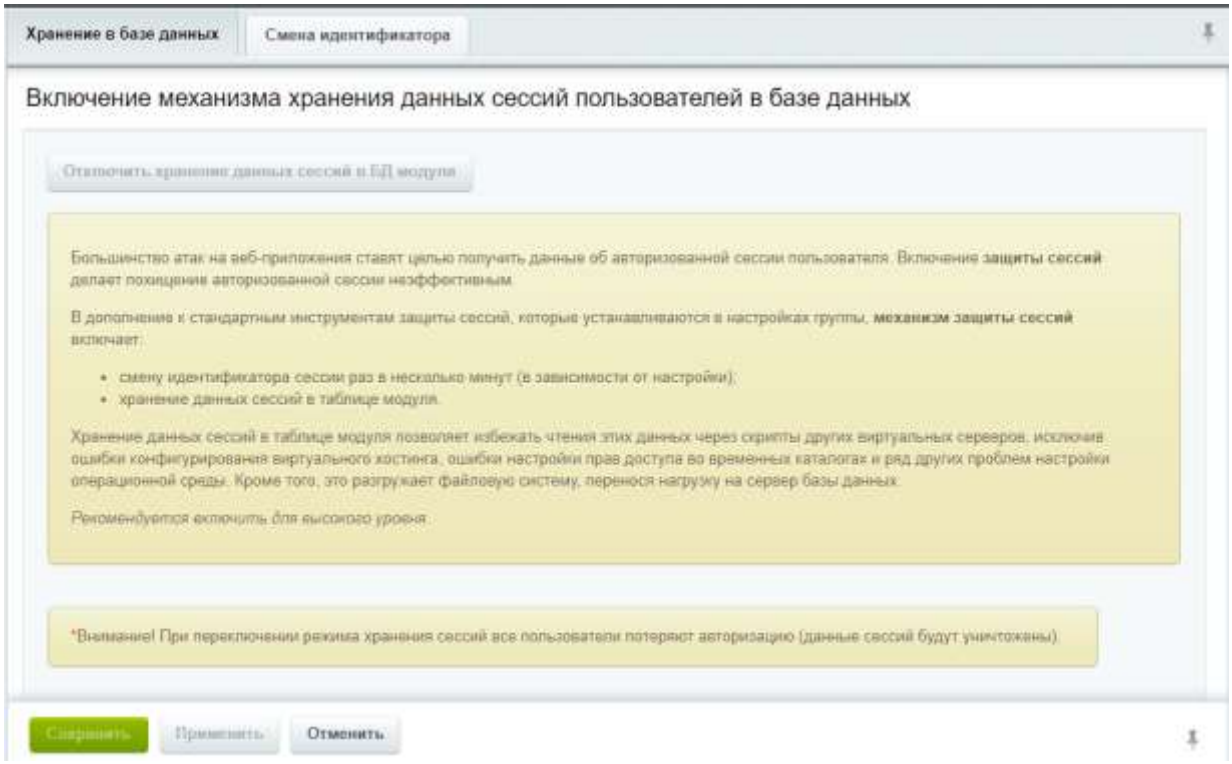



Рисунок 2.13 – Результат перевірки користувача групи «Адміністратор інтернет-магазину» на можливість користування елемента модуля «Проактивний захист»

Таблиця 2.1 – Рівні доступу груп користувачів до кожного функціонального модулю

| Модуль, права доступу | Адміні-стратори | Усі користувачі (у тому числі не авторизовані) | Зареєстровані користувачі | Адміні-стратори інтернет-магазину | Контент-редактори |
|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 |
| Головний модуль | Повний доступ | Закритий | Зміна свого профілю | Повний доступ до управління інтернет-магазином і параметрами торгового каталогу | Зміна свого профілю |
| Email-маркетинг | Повний доступ | Закритий | | | |
| Блоги | Повний доступ | Читання блогів | | | |
| Валюти | Повний доступ | Закритий | | | |
| Веб-форми | Повний доступ | Закритий | | | |
| Інтеграція з Бітрікс24 | Повний доступ | Закритий | | | |

Продовження табл.2.1

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| Інтернет магазин | Повний доступ | Закритий | | Обробка замовлень | Закритий |
| Торговий каталог | Повний доступ | Закритий | | Редагування цін | Закритий |
| Монітор продукти-вності | Повний доступ | Закритий | | | |
| Хмарні сховища | Повний доступ | Закритий | | | |
| Опиту-вання, голосува-ння | Повний доступ | Закритий | | | |
| Переклад | Повний доступ | Закритий | | | |
| Підписка, розсилки | Повний доступ | Закритий | | | |
| Пошукова оптимізація | Повний доступ | Закритий | | | |
| Проактивний захист | Повний доступ | Закритий | | Перегляд усіх даних | Закритий |
| Сайти 24 | Повний доступ | Заборонено | | | |
| Торговий каталог | Повний доступ | Закритий | | | |
| Управління структурою | Повний доступ | Закритий | | | |

Продовження табл.2.1

| 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|
| Форум | Повний доступ | Закритий | | | |
| A / B-тестування | Повний доступ | Закритий | | | |
| Конверсія | Повний доступ | Закритий | | Запис | Закритий |
| Майстер магазину | Повний доступ | Закритий | | Запис | Закритий |
| Мобільний додаток для інтернет-магазину | Повний доступ | Закритий | | Перегляд усіх даних модулю | Закритий |
| Служба повідомлень | Повний доступ | Закритий | | | |
| Мобільна платформа | Повний доступ | Закритий | | | |
| Push and Pull | Повний доступ | Закритий | | | |

## 2.6 Програма і методика випробувань функціональної послуги безпеки «Реєстрація» рівня HP-1 – «Зовнішній аналіз»

### 2.6.1 Програма випробувань

– Перевірка послуги, що визначає перелік реєстраційних подій пов'язаних зі спробами, або фактами виконання певних дій, що мають

безпосереднє або непряме відношення до безпеки оброблюваної інформації, реєстрація яких можлива засобами, реалізованими у складі системи «Бітрікс: Управління сайтом».

– Перевірка здатності здійснення реєстрації подій, що мають безпосереднє відношення до безпеки.

– Перевірка журналу реєстрації, щодо розміщення в ньому інформації про дату, час, місце, тип і успішність та неуспішність кожної зареєстрованої події.

– Перевірка журналу реєстрації, щодо структури його записів, які повинні містити інформацію, достатню для встановлення користувача, процесу та/або об’єкта, що мали відношення до кожної зареєстрованої події.

– Перевірка атрибутів користувачів, що зберігаються в журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, щодо автентифікації, з використанням засобів реалізації послуги «Ідентифікація та автентифікація» рівня НИ-2.

– Перевірка здатності передачі журналу реєстрації в інші системи з використанням певних механізмів захисту переданого журналу від несанкціонованого доступу з метою модифікації або руйнування.

### 2.6.2 Методика випробувань

– Перевірка атрибутів користувачів, що зберігаються в журналі реєстрації та на підставі яких приймається рішення про відношення користувача до зареєстрованої події, щодо автентифікації, з використанням засобів реалізації послуги «Ідентифікація та автентифікація» рівня НИ-2.

1) Перевіряється всі типи користувачів, атрибути яких зберігаються в журналі реєстрації, щодо попереднього виконання випробувань засобів реалізації послуги безпеки «Ідентифікація та автентифікація» рівня НИ-2. Повинні бути виконані випробування засобів реалізації послуги безпеки

«Ідентифікація та автентифікація» рівня НИ-2 для кожного типу користувачів, атрибути яких зберігаються в журналі реєстрації.

– Перевірка пунктів 1, 2, 6 програми випробувань.

1) Перевіряється виконання запитів та інших дій, результатами яких є факти реєстрації кожної з подій, з подальшим виконанням передачі журналу реєстрації в інші системи та аналізується переданий журнал реєстрації в інших системах на предмет наявності записів про всі зареєстровані події. Усі запити та події повинні виконуватися з подальшою передачею журналу в інші системи.

– Перевірка здатності передачі журналу реєстрації в інші системи з використанням певних механізмів захисту переданого журналу від несанкціонованого доступу з метою модифікації або руйнування.

1) Перевіряється виконання спроб модифікації або руйнування переданого в інші системи журналу, що містить події, зареєстровані при виконанні перевірок. Виконання спроб модифікації або руйнування журналу повинні бути не ефективними.

2) Аналізується журнал у цих системах з використанням відповідних засобів на предмет наявності записів про зареєстровані події. Записи у журналі повинні бути збережені.

– Перевірка пунктів 1, 3, 4 програми випробувань.

1) Аналізується, переданий в іншу систему журнал, на предмет наявності в записах журналу інформації про дату, час, місце, тип і успішність кожної зареєстрованої події. Інформація в записах журналу про дату, час, місце, тип і успішність кожної зареєстрованої події повинна бути в наявності.

2) Аналізується переданий в іншу систему журнал на предмет наявності в записах журналу інформації, достатньої для установлення користувача, процесу та/або об’єкта, що мали відношення до зареєстрованої події. У записах журналу повинна бути інформація достатня для установлення користувача, процесу та/або об’єкта, що мали відношення до зареєстрованої події.

2.6.3 Результати випробування

Виконання перевірки функціональної послуги безпеки «Ідентифікація та автентифікація» рівня НИ-2 – «Одиночна ідентифікація та автентифікація» показана в пункті 2.4.3.

Перевірено виконання спроби атаки через XSS та впровадження вірусу, що було зареєстровано для кожної з подій, що показано на рис 2.14.

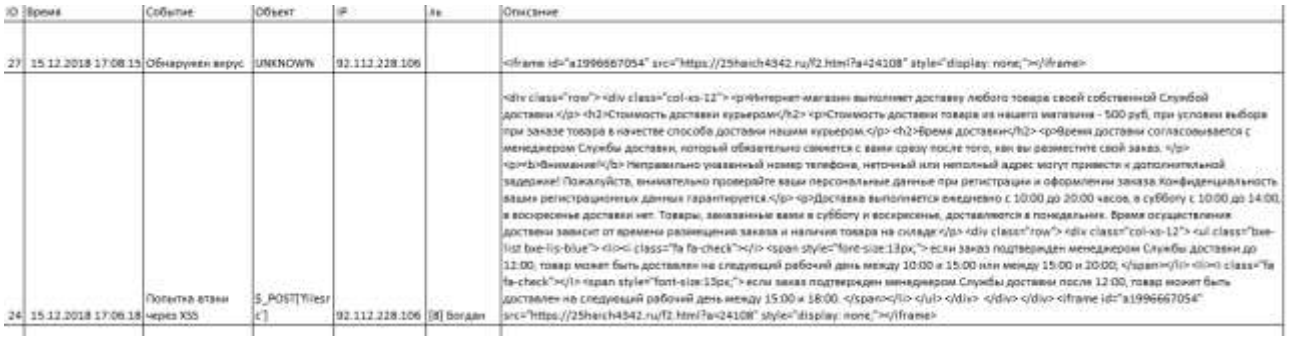
| ID | Время | Событие | Объект | IP | Пользователь | Описание |
|---|---|---|---|---|---|---|
| 27 | 15.12.2018 17:08:15 | Обнаружен вирус | UNKNOWN | 92.112.228.106 | | <iframe id="a1996667054" src="https://25halch4342.ru/f2.html?a=24100" style="display: none;"></iframe> |
| 24 | 15.12.2018 17:06:18 | Попытка атаки через XSS | $_POST['filename'] | 92.112.228.106 | [ID] Богдан |   Интернет-магазин выполняет доставку любого товара своей собственной Службой доставки. <h2>Стоимость доставки курьером</h2> Стоимость доставки товара из нашего магазина - 500 руб. при условии выбора при заказе товара в качестве способа доставки нашим курьером. <h2>Время доставки</h2> Время доставки согласовывается с менеджером Службы доставки, который обязательно свяжется с вами сразу после того, как вы разместите свой заказ.  Внимание! Неправильно указанный номер телефона, неточный или неполный адрес могут привести к дополнительной задержке! Пожалуйста, внимательно проверяйте ваши персональные данные при регистрации и оформлении заказа.Конфиденциальность ваших регистрационных данных гарантируется. Доставка выполняется ежедневно с 10:00 до 20:00 часов, в субботу с 10:00 до 14:00, в воскресенье доставки нет. Товары, заказанные вами в субботу и воскресенье, доставляются в понедельник. Время осуществления доставки зависит от времени размещения заказа и наличия товара на складе.   <ul class="bxe-list bxe-ils-blue"> <li>  если заказ подтвержден менеджером Службы доставки до 12:00, товар может быть доставлен на следующий рабочий день между 10:00 и 15:00 или между 15:00 и 20:00. </li> <li>  если заказ подтвержден менеджером Службы доставки после 12:00, товар может быть доставлен на следующий рабочий день между 15:00 и 18:00. </li> </ul>  |

Рисунок 2.14 – Записи журналу подій

Виявлення, блокування та передачу в журнал даних про спроби атаки виконано «Проактивним фільтром (Web Application Firewall)».

Виявлення, оповіщення адміністратора та передачу в журнал даних про спроби впровадження вірусу виконано «Веб-антивірусом».

Потім було перевірено передачу журналу в іншу систему (у даному випадку передачу на комп’ютер адміністратора) у файлі формату .xls та перевірено дані, що знаходяться у ньому. Усі записи про всі зареєстровані події у наявності. У записах журналу є інформація про дату, час, місце, тип і успішність кожної зареєстрованої події, а також інформація, достатня для установлення користувача, процесу та/або об’єкта, що мали відношення до зареєстрованої події, що показано на рисунку 2.15



| ID | Время | Событие | Объект | IP | Ав | Описание |
|---|---|---|---|---|---|---|
| 27 | 15.12.2018 17:08:15 | Обнаружен вирус | UNKNOWN | 92.112.228.106 | | <iframe id="a1996667054" src="https://25haich4342.ru/f2.html?a=24108" style="display: none;"></iframe> |
| 24 | 15.12.2018 17:08:18 | Попытка атаки через XSS | $_POST['files'] | 92.112.228.106 | [8] Богдан |   Интернет-магазин выполняет доставку любого товара своей собственной Службой доставки  <h2>Стоимость доставки курьером</h2> Стоимость доставки товара из нашего магазина - 500 руб, при условии выбора при заказе товара в качестве способа доставки нашим курьером. <h2>Время доставки</h2> Время доставки согласовывается с менеджером Службы доставки, который обязательно свяжется с вами сразу после того, как вы разместите свой заказ.  Внимание! Неправильно указанный номер телефона, неточный или неполный адрес могут привести к дополнительной задержке! Пожалуйста, внимательно проверяйте ваши персональные данные при регистрации и оформлении заказа.Конфиденциальность вашим регистрационных данных гарантируется. Доставка выполняется ежедневно с 10:00 до 20:00 часов, в субботу с 10:00 до 14:00, в воскресенье доставки нет. Товары, заказанные вами в субботу и воскресенье, доставляются в понедельник. Время осуществления доставки зависит от времени размещения заказа и наличия товара на складе.   <ul class="bxe-list bxe-list-blue"> <li> если заказ подтвержден менеджером Службы доставки до 12:00, товар может быть доставлен на следующий рабочий день между 10:00 и 15:00 или между 15:00 и 20:00; </li> <li> если заказ подтвержден менеджером Службы доставки после 12:00, товар может быть доставлен на следующий рабочий день между 15:00 и 18:00. </li> </ul>   <iframe id="a1996667054" src="https://25haich4342.ru/f2.html?a=24108" style="display: none;"></iframe> |

Рисунок 2.15 – Записи журналу подій в операційній системі у файлі .xls

У даній роботі перевірка виконання спроб модифікації або руйнування переданого в інші системи журналу, що містить події, зареєстровані при виконанні перевірок не виконана через те, що це не входить у функції «Проактивного захисту».

2.7 Програма і методика випробувань функціональної послуги безпеки «Конфіденційність при обміні» рівня КВ-1 – «Мінімальна конфіденційність при обміні»

2.7.1 Програма випробувань

– Перевірка того, що політика послуги, що реалізує КЗЗ відноситься до паролів.

– Перевірка того, що політика послуги, що реалізує КЗЗ визначає рівень захищеності.

– Перевірка забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в переданих об’єктах (паролях) з використанням “безпечної авторизації” модулю «Проактивний захист».

### 2.7.2 Методика випробувань

– Перевірка пунктів 1, 2, 3 програми випробувань.

1) Перевірка спроби передачі і приймання об’єктів (паролів) з подальшим аналізом вмісту переданих і прийнятих об’єктів з метою підтвердження можливості забезпечення захисту від безпосереднього ознайомлення з інформацією, що міститься в переданих об’єктах. При передачі і прийманні об’єктів повинен забезпечуватися захисту від ознайомлення з інформацією.

### 2.7.3 Результати випробування

Для захисту даних при передачі паролів використовується «безпечна авторизація», завдяки якій паролі з форми авторизації шифруються за алгоритмом RSA з ключем 1024 біт і в такому вигляді передаються на сервер. Для підключення «безпечної авторизації» потрібно її увімкнути в налаштуваннях головного модулю, що показано на рисунку 2.16.

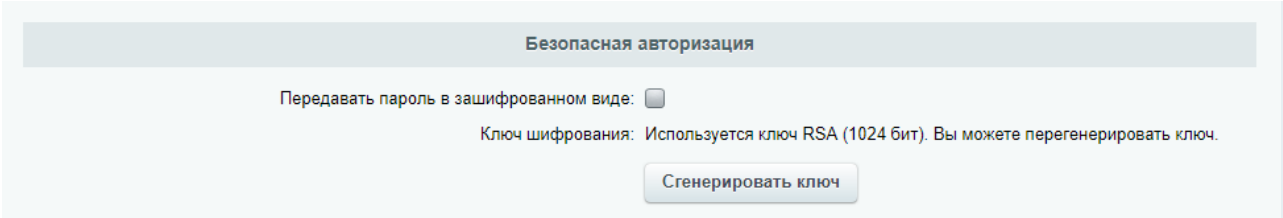



Рисунок 2.16 – Панель увімкнення шифрування паролів

При перевірці автентифікації користувача без використання “безпечної авторизації” було встановлено, що пароль передається на сервер у відкритому вигляді, що показано на рисунку 2.17.

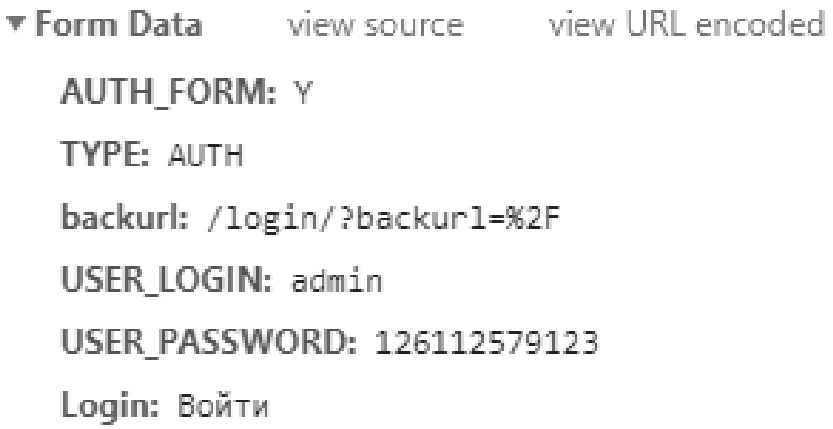



Рисунок 2.17 – Дані відправки форми без шифрування пароля

При перевірці автентифікації користувача з використанням “безпечної авторизації” було встановлено, що пароль передається на сервер у зашифрованому вигляді, що показано на рисунку 2.18


Рисунок 2.18 – Дані відправки форми з шифруванням пароля

Таким чином для захисту даних при передачі у модулі «проактивний захист» використовується шифрування паролів алгоритмом RSA з ключем 1024 біт.

## 2.8 Програма і методика випробувань функціональної послуги безпеки «Цілісність комплексу засобів захисту» рівня НЦ-1 – «КЗЗ з контролем цілісності»

### 2.8.1 Програма випробувань

– Перевірка, що політика послуги визначає склад КЗЗ та механізми контролю цілісності всіх компонентів, що входять до складу КЗЗ.

– Перевірка, що у випадку виявлення засобами контролю цілісності, порушення цілісності будь-якого зі своїх компонентів, КЗЗ здатний зареєструвати факт порушення, за допомогою засобів реалізації послуги «Реєстрація» рівня НР-1, повідомити адміністратора, автоматично відновити відповідність компонента еталону, або перевести КЗЗ у стан, з якого повернути його до нормального функціонування може лише адміністратор, або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1.

– Перевірка обмежень, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об’єктів контролюється КЗЗ.

### 2.8.2 Методика випробувань

– Перевірка, що у випадку виявлення засобами контролю цілісності, порушення цілісності будь-якого зі своїх компонентів, КЗЗ здатний зареєструвати факт порушення, за допомогою засобів реалізації послуги «Реєстрація» рівня НР-1, повідомити адміністратора, автоматично відновити відповідність компонента еталону, або перевести КЗЗ у стан, з якого повернути його до нормального функціонування може лише адміністратор, або користувачі, яким надані відповідні повноваження і які відносяться до певних

ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1;

1) Перевіряється виконання випробувань реалізації функціональної послуги безпеки «Розмежування обов'язків» рівня НО-1. Реалізації функціональної послуги безпеки «Розмежування обов'язків» рівня НО-1 повинна виконуватися.

– Перевірка пунктів 1, 2 програми випробувань.

1) Перевіряється виконання почергової модифікації кожного з компонентів КЗЗ, перед їх запуском з контролем виявлення порушення цілісності. При виконанні почергової модифікації кожного з компонентів КЗЗ, перед їх запуском повинне виявлятися порушення цілісності.

2) Перевіряється виконання почергової модифікації кожного з компонентів КЗЗ, перед їх запуском з контролем оповіщення адміністратора про виявлені факти порушення цілісності. Виконання почергової модифікації кожного з компонентів КЗЗ, перед їх запуском повинне оповіщатися адміністратору про виявлені факти порушення цілісності.

3) Перевіряється виконання почергової модифікації кожного з компонентів КЗЗ, перед їх запуском з контролем реєстрації відповідних подій засобами «Реєстрація» рівня НР-1. Виконання почергової модифікації кожного з компонентів КЗЗ, перед їх запуском повинне реєструватись відповідними подіями засобами «Реєстрація» рівня НР-1.

4) Перевіряється виконання почергової модифікації кожного з компонентів КЗЗ, перед їх запуском з контролем автоматичного відновлення відповідності компонента еталону або переведення в стан, з якого повернути його до нормального функціонування може лише адміністратор, або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1. При виконанні почергової модифікації кожного з компонентів КЗЗ, перед їх запуском повинне відбуватися автоматичне відновлення відповідності компонента еталону або переведення в стан, з якого повернути його до

нормального функціонування може лише адміністратор, або користувачі, яким надані відповідні повноваження і які відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов’язків» рівня НО-1.

5) Перевіряються засоби реалізації послуги «Реєстрація», механізми і засоби оповіщення адміністраторів про виявлені факти порушення цілісності, засоби автоматичного відновлення відповідності зруйнованих компонентів КЗЗ еталону. Повинна виконуватися реалізації послуги «Реєстрація».

– Перевірка обмежень, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і всі запити на доступ до захищених об’єктів контролюється КЗЗ.

1) Аналізуються обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і запити на доступ до захищених об’єктів контролюється КЗЗ.

### 2.8.3 Результати випробування

Виконання перевірки функціональної послуги безпеки «Розмежування обов'язків» рівня НО-1– «Виділення адміністратора» показана в пункті 2.5.3.

Перевірено, що при спробі модифікації кожного з компонентів КЗЗ, перед їх запуском відбувається переведення в стан, з якого повернути його до нормального функціонування може лише адміністратор, що показано на рисунку 2.19

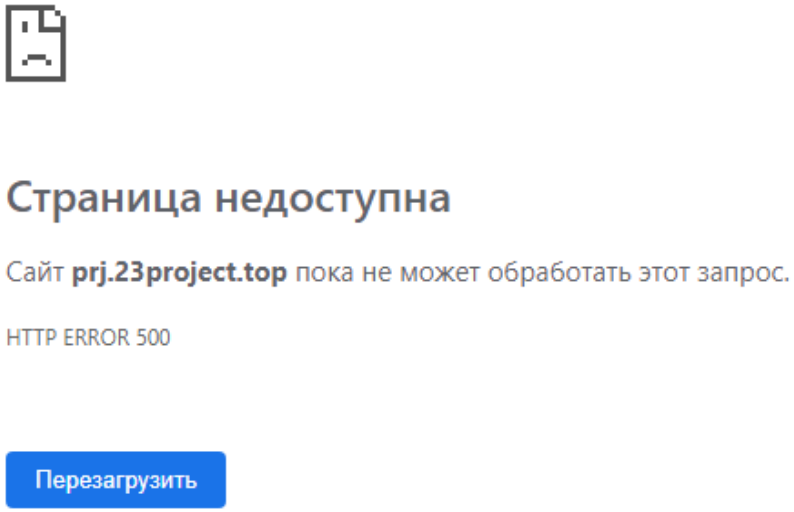



Рисунок 2.18 – Відображення на веб-сторінці сайту

Для перевірки цілісності файлів використовується «Контроль цілісності файлів». «Контроль цілісності скрипта» дозволяє зробити перевірку цілісності файлів, що показано на рисунку 2.19

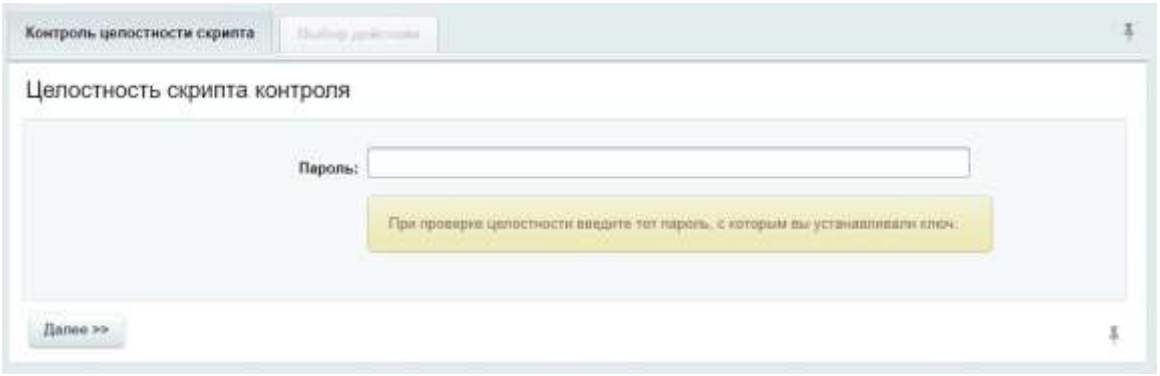



Рисунок 2.19 – Елемент захисту «Контроль цілісності скрипта»

Після уведення паролю є можливість переглянути звіт цілісності файлів щодо змін після попередньої перевірки, що показано на рисунку 2.20

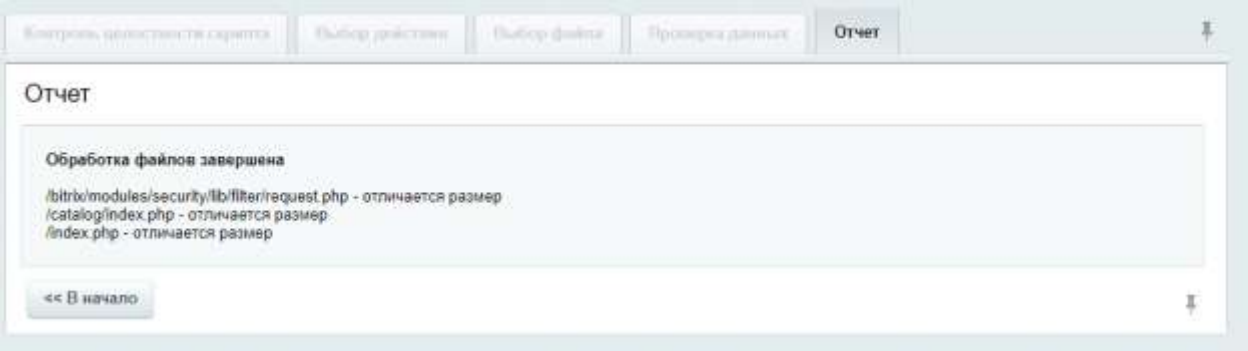



Рисунок 2.20 – Звіт перевірки цілісності файлів

Одним з обмежень, що реалізується «Проактивним захистом» є «Захист адміністративних розділів по IP» що дозволяє гарантувати, що послуги безпеки доступні лише через інтерфейс КЗЗ і запити на доступ до захищених об’єктів контролюється КЗЗ.

Контроль виявлення порушення цілісності КЗЗ, оповіщення адміністратора про виявлені факти порушення цілісності КЗЗ, реєстрація порушення цілісності КЗЗ засобами «Реєстрація» не реалізується елементами модуля «Проактивний захист», тому в даній роботі не розглядаються.

## 2.9 Програма і методика випробувань функціональної послуги безпеки «Самотестування» рівня НТ-1 – «Самотестування за запитом»

### 2.9.1 Програма випробувань

– Перевірка властивостей системи «Бітрікс: Управління сайтом» та реалізованих процедур що можуть бути використані для оцінювання правильності функціонування КЗЗ.

– Перевірка того, що КЗЗ здатний, з використанням засобів, виконувати набір тестів з метою оцінювання правильності функціонування своїх критичних функцій за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1.

### 2.9.2 Методика випробувань

– Перевірка того, що КЗЗ здатний, з використанням засобів, виконувати наведений набір тестів з метою оцінювання правильності функціонування своїх критичних функцій за запитом користувачів, що мають відповідні повноваження та відносяться до певних ролей згідно з політикою реалізованої КЗЗ послуги «Розмежування обов'язків» рівня НО-1.

1) Перевіряється виконання випробувань засобів реалізації функціональної послуги безпеки «Розмежування обов'язків» рівня «НО-1». Реалізації функціональної послуги безпеки «Розмежування обов'язків» рівня «НО-1» повинна виконуватися.

– Перевірка властивостей системи «Бітрікс: Управління сайтом» та реалізованих процедур що можуть бути використані для оцінювання правильності функціонування КЗЗ;

1) Перевіряється виконання, з використанням відповідних засобів випробувань, почергової імітації непрацездатності кожного з компонентів, що входять до складу КЗЗ, з подальшим ініціюванням виконання наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів та контролю результатів виконання різних тестів. Перевіряється виконання, з використанням відповідних засобів випробувань, імітації непрацездатності компонентів системи, що входять до складу КЗЗ з подальшим ініціюванням виконання, з використанням засобів наборів тестів, використовуваних для оцінювання правильності функціонування відповідних компонентів та контролю результатів виконання різних тестів. Тести повинні виконуватися для оцінювання правильності функціонування відповідних компонентів.

### 2.9.3 Результати випробування

Виконання перевірки функціональної послуги безпеки «Розмежування обов'язків» рівня НО-1– «Виділення адміністратора» показана в пункті 2.5.3.

Для виконання тестів системи використовуються такі засоби тестування: «Сканер безпеки», та «Інструмент для аудиту безпеки PHP-коду».

Перевірено, що за допомогою «Сканера безпеки» виконуються набір тестів для перевірки системи, що показано на рисунку 2.21.

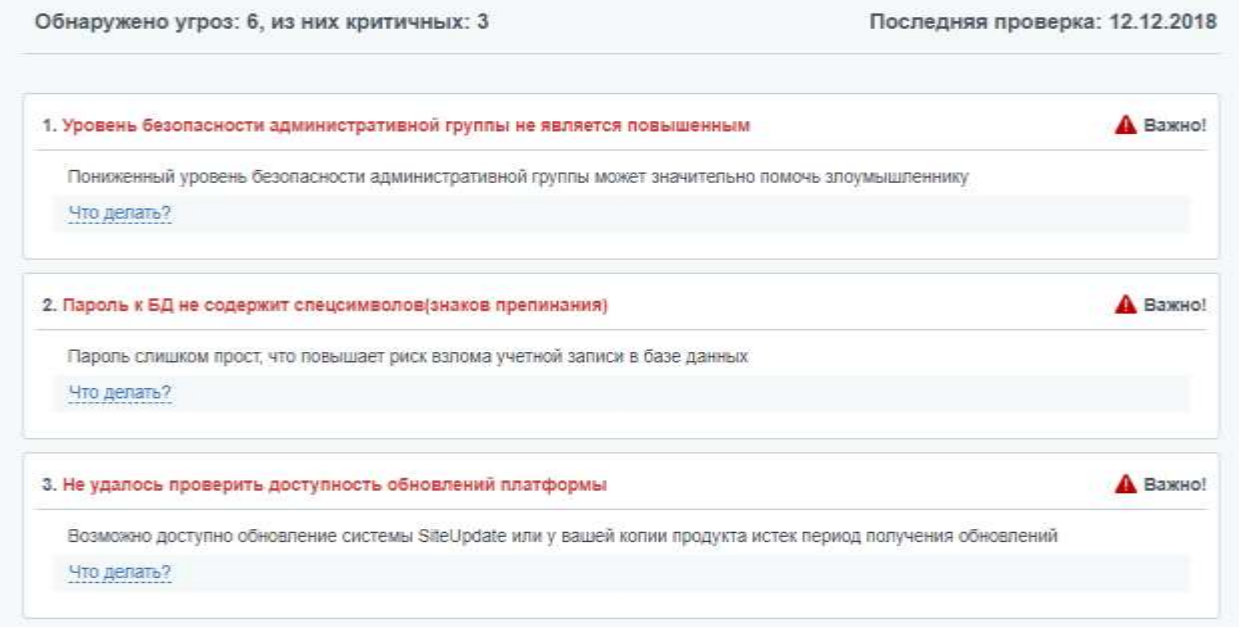



Рисунок 2.21 – Загрози виявлені «Сканером безпеки»

Додатковим інструментом перевірки є «Інструмент для аудиту безпеки PHP-коду», який виконує перевірку коду на можливі вразливості. Виявлення вразливості до XSS зображено на рисунку 2.21

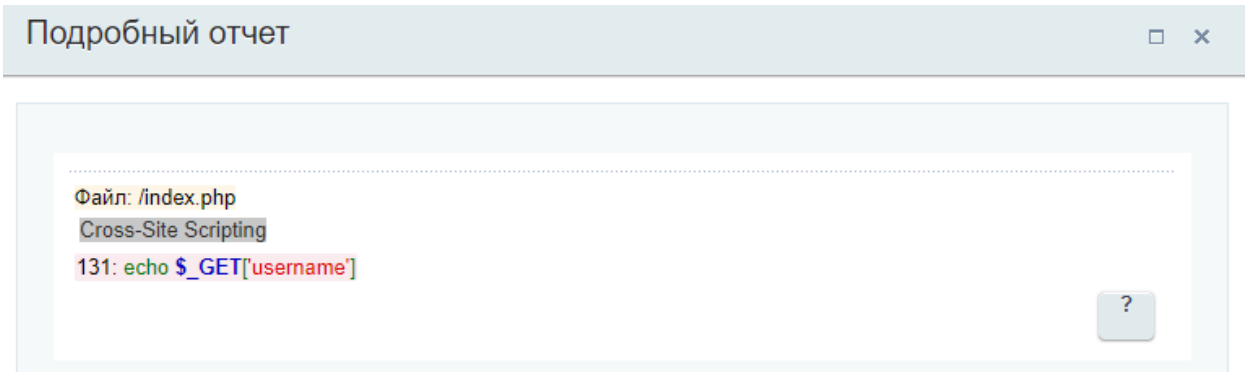



Рисунок 2.22 – Звіт «Інструмента для аудиту безпеки PHP-коду»

Таким чином, тести виконуються для оцінювання правильності функціонування відповідних компонентів.

## 2.10 Висновки до другого розділу

Оскільки до переліку засобів ТЗІ дозволених для забезпечення технічного захисту державних інформаційних ресурсів входить система «Бітрікс: Управління сайтом» версії 15.х, а її експертний висновок на разі не є дійсним, то для доказу захищеності системи потрібно робити перевірку самостійно. Розроблена у дипломній роботі програма та методика проведення аналізу рівня захищеності системи «Бітрікс: Управління сайтом» версії 18.х допоможе перевіряючому провести експертизу системи захисту з використанням системи «Бітрікс: Управління сайтом» версії 18.х.

У даній роботі виконано перевірку виконання функціональних послуг безпеки, що повинні забезпечуватися завдяки модулю «Проактивний захист»:

- НК – достовірний канал;
- НИ – ідентифікація і автентифікація;
- НО – розподіл обов'язків;
- НР – реєстрація;
- КВ – конфіденційність при обміні;
- НЦ – цілісність КЗЗ;
- НТ – самотестування.

Технічні вимоги щодо захисту інформації, що забезпечується модулем «Проактивний захист», від несанкціонованого доступу, сукупність яких визначається функціональним профілем: КВ-1, НР-1, НИ-2, НК-1, НО-1, НЦ-1, НТ-1.

Рівні перевіряючих послуг:

- КВ-1 – «Мінімальна конфіденційність при обміні».
- НР-1 – «Зовнішній аналіз».
- НИ-2 – «Одиночна ідентифікація та автентифікація».
- НК-1 – «Однонаправлений достовірний канал».
- НО-1 – «Виділення адміністратора».

– НЦ-1 – «КЗЗ з контролем цілісності».

– НТ-1 – «Самотестування за запитом»

Для повної перевірки системи потрібно перевіряти й інші функціональні послуги безпеки.

# РОЗДІЛ 3. ЕКОНОМЧНЕ ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ СТВОРЕННЯ ПРОГРАМИ ТА МЕТОДИКИ ПРОВЕДЕННЯ АНАЛІЗУ РІВНЯ ЗАХИЩЕНОСТІ СИСТЕМИ «БІТРІКС: УПРАВЛІННЯ САЙТОМ» ВЕРСІЇ 18.X

## 3.1 Вступ

Метою розділу є обгрунтування економічної доцільності створення програми та методики проведення аналізу рівня захищеності системи «Бітрікс: Управління сайтом» версії 18.x

Для забезпечення захисту веб-додатку потрібно користуватись експертним висновком переліку засобів ТЗІ дозволених для забезпечення технічного захисту державних інформаційних ресурсів, або довести ефективність захисту веб-додатку. Для доказу захисту системи «Бітрікс: Управління сайтом» було створено програму та методику проведення аналізу рівня захищеності.

Щоб визначити ефективність необхідно розрахувати:

– капітальні витрати на розробку, впровадження та підтримку створення програми та методики;

– трудомісткість витрати на розробку, впровадження та підтримку програми та методики а також трудомісткість на підтримку системи «Бітрікс: Управління сайтом»;

– річні експлуатаційні витрати на впровадження та підтримку системи «Бітрікс: Управління сайтом»;

– показники економічної ефективності захисту веб-додатка завдяки застосуванню програми та методики в організації.

3.2 Розрахунок фіксованих (капітальних) витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Витрати на створення програми і методики $К_{пз}$ складаються з витрат на заробітну плату виконавця програми і методики $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання на ПК $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч} \quad (3.1)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальні потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{ЗП} = t \cdot З_{ПР}, \quad \text{грн}, \quad (3.2)$$

де t – загальна тривалість створення ПЗ, годин;

$З_{пр}$ – средньогодинна заробітна плата.

Розрахуємо час, який буде витрачено на створення програми і методики:

$$t = t_{тз} + t_{втз} + t_{ае} + t_{сп} + t_{вз} + t_{ор}, \text{ годин}, \quad (3.3)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку програми та методики;

$t_{втз}$ – тривалість вивчення технічного завдання;

$t_{ае}$ – тривалість аналізу елементів модуля «Проактивний захист» системи «Бітрікс: Управління сайтом»;

$t_{сп}$ – тривалість складання програми та методики проведення аналізу рівня захищеності системи «Бітрікс: Управління сайтом»;

$t_{вз}$ – тривалість випробувань захищеності системи «Бітрікс: Управління сайтом»;

$t_{ор}$ – тривалість опрацювання результатів;

У таблиці 3.1 представлена трудомісткість процесів.

Таблиця 3.1 – Трудомісткість процесів

| Назва процесу | Трудомісткість, год. |
|---|---|
| Складання технічного завдання на розробку програми та методики | 16 |
| Вивчення технічного завдання | 8 |
| Аналіз елементів модуля «Проактивний захист» системи «Бітрікс: Управління сайтом» | 64 |
| Складання програми та методики проведення аналізу рівня захищеності системи «Бітрікс: Управління сайтом» | 56 |
| Випробування захищеності системи «Бітрікс: Управління сайтом» | 152 |
| Опрацювання результатів | 80 |

$$t = 16 + 8 + 56 + 56 + 136 + 64 = 376 \text{ годин.}$$

$З_{пр}$ – середньогодинна заробітна плата фахівця з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_м}{t_m} = \frac{15000}{160} = 93{,}75, \text{ грн/год,} \quad (3.4)$$

де $З_м$– середня заробітна плата фахівця з інформаційної безпеки – 15 000 грн., $t_m$ – робочій час на місяць -160 год.

$$З_{зп} = 376 \cdot 93{,}75 = 35\,250, \text{ грн}$$

Вартість машинного часу для впровадження програми і методики визначається за формулою:

$$З_{мч} = (t_{опр} \cdot C_{мч} + t_д), \text{ грн,} \quad (3.5)$$

де $t_{опр}$ – трудомісткість налагодження всіх необхідних операцій на ПК, годин (80 год);

$t_д$ – трудомісткість підготовки документації на Пк, годин (40 год);

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p}, \text{ грн} \quad (3.6)$$

де $P$ – встановлена потужність ПК, 0.5 кВт;

$C_e$ – тариф на електричну енергію, 1.68 грн/кВт·година;

$Ф_{зал}$– залишкова вартість ПК на початок року, 7000 грн.;

$H_a$ – річна норма амортизації на ПК, 0.1 частки одиниці;

$F_p$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_p$ = 1920 год).

$$C_{мч} = 0{,}5 \cdot 1{,}68 + \frac{7000 \cdot 0{,}1}{1920} = 1{,}20, \text{ грн/год}$$

$$З_{мч} = 80 \cdot 1{,}20 + 40 = 136 \text{ грн.}$$

Таким чином, капітальні (фіксовані) витрати на створення та впровадження програми та методики складають:

$$К_{пз} = 136+31\ 500 = 31\ 636, \text{ грн} \quad (3.7)$$

Оскільки в даній роботі розглядається тільки перевірка елементів захисту модуля «Проактивний захист», перевірка повної системи вимагає більше часу, а відповідно більші капітальні витрати. Пердбачається, що для повної перевірки капітальні витрати становитимуть у 2 рази більше.

## 3.3 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Річні поточні (експлуатаційні) витрати на функціонування системи інформаційної безпеки складають:

$$С = С_а + С_з + С_{ел} + С_{тос}, \text{ грн}, \quad (3.8)$$

де $С_а$ – річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ);

$$С_а = К_{пз} /2 =(31\ 636)/2=15\ 818, \text{ грн}, \quad (3.9)$$

Сз – річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ,складає:

$$С_з = (Зм+ 22\%) \cdot m = 15\ 000 \cdot 12 = 180\ 000 \text{ грн} , \quad (3.10)$$

де m – кількість місяців.

До річного фонду заробітної плати додається єдиний внесок (22%) на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

Розмір єдиного внеску на загальнообов'язкове державне соціальне страхування визначається на підставі встановленого чинним законодавством відсотка від суми основної та додаткової заробітної плати

$С_{ел}$ – вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року, визначається за формулою:

$$С_{ел} = Р \cdot Fр \cdot Ц_е , \text{ грн}, \quad (3.11)$$

де Р – встановлена потужність апаратури інформаційної безпеки, 0.5 кВт;

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (за 40-годинного робочого тижня $F_р$ = 2080 год);

$Ц_е$ – тариф на електроенергію, грн/кВт·годин, 1.68 грн/кВт·година.

$$С_{ел} = 0,5 \cdot 2080 \cdot 1,68 = 1\,747,2 \text{ грн.}$$

$С_{тос}$ – витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначається за формулою:

$$С_{тос} = С_{ліц} + С_{хст}, \text{ грн}, \quad (3.12)$$

де $С_{ліц}$ – вартість ліцензії на 1 рік системи «Бітрікс: Управління сайтом»*;*

$С_{хст}$ – вартість послуги хостинга на 1 рік.

$$С_{тос} = 7\ 100 + 1\ 479 = 8\ 579, \text{ грн}$$

Отже, річні поточні (експлуатаційні) витрати складають:

$$С = 15\ 818 + 180\ 000 + 1\ 747{,}2 + 8\ 579 = 206\ 144{,}2 \text{ грн.}$$

3.4 Оцінка можливого збитку від атаки

Упущена вигода від простою атакованого вузла або сегмента системи становить:

$$U = П_п + П_в + V, \quad (3.13)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента системи, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента системи (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента системи, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зс}{F} \cdot t_П \ , \quad (3.14)$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч);

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, грн на місяць;

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин.

$$П_п = \frac{15000 + 12000}{176} \cdot 2 = 306,82 \text{ , грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв}, \quad (3.15)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента системи $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ВИ} = \frac{\sum Зс}{F} \cdot t_{ВИ} \text{ , } \quad (3.16)$$

де $t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$$П_{ви} = \frac{5000 + 5000 + 12000}{176} \cdot 4 = 500 \text{ , грн}$$

Витрати на відновлення вузла або сегмента системи $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в \ , \qquad (3.17)$$

де Зо – заробітна плата обслуговуючого персоналу (адміністратора), грн на місяць;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин.

$$П_{пв} = \frac{15000}{176} \times 2 = 170{,}46 \text{ , грн}$$

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = 500 + 170{,}46 = 670{,}46, \text{ грн}$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента системи визначаються виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{О}{Fг} \cdot (t_П + t_В + t_{ВИ}) \ , \qquad (3.18)$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч;

О – обсяг продажів атакованого вузла або сегмента корпоративної мережі, грн у рік.

$$V=\frac{750000}{2080}\times(2+4+2)=2884{,}64 \text{ , грн}$$

Упущена вигода від простою атакованого вузла або сегмента системи становить:

$$U = 306{,}82 + 670{,}46 + 2\ 884{,}64 = 3\ 861{,}92 \text{ , грн}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum_i \sum_n U, \qquad (3.19)$$

де i – число атакованих вузлів або сегментів системи;

n – середнє число атак на рік.

$$B = 1 \cdot 450 \cdot\ 3\ 861{,}92 = 1\ 737\ 864 \text{ грн.}$$

3.5 Загальний ефект від використання засобів безпеки, які дозволено використовувати завдяки програмі та методиці

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \qquad (3.20)$$

де В – загальний збиток від атаки на вузол або сегмент корпоративної мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці(0,4 найбільш ймовірній відсоток);

С – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

$$E = 1\,737\,864 \cdot 0{,}4 - 206\,144{,}2 = 489\,001{,}4 \text{ грн.}$$

## 3.6 Економічне обгрунтування

Оцінка економічної ефективності системи захисту інформації, здійснюється на основі визначення та аналізу наступних показників:

– коефіцієнт повернення інвестицій (ROI). У сфері інформаційної безпеки йому відповідає показник ROSI (Return on Investment for Security);

– термін окупності капітальних інвестицій $T_o$.

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки.

Щодо до інформаційної безпеки говорять не про прибуток, а про запобігання можливих втрат від атаки на сегмент або вузол корпоративної мережі, а отже:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \qquad (3.21)$$

де Е – загальний ефект від впровадження системи інформаційної безпеки, грн;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

$$ROSI = \frac{489001,4}{31636} = 15$$

Нормативне значення коефіцієнта повернення інвестицій визначається з наступних міркувань.

Організація здійснює фінансування капітальних інвестицій за рахунок реінвестування власних коштів (частини прибутку та амортизаційних відрахувань), то в якості $E_н$ варто приймати бажану норму прибутковості альтернативних варіантів вкладення коштів К (наприклад, у цінні папери, інші проекти, на депозитний рахунок у банку, тощо) з урахуванням інфляції. Визначити бажане значення коефіцієнта ефективності можна також виходячи з прийнятної для підприємства індивідуальної норми прибутковості, яка б, принаймні, не знижувала ринкову вартість фірми.

При цьому проект визнається економічно доцільним, якщо розрахунковий коефіцієнт ефективності перевищує річний рівень прибутковості альтернативного варіанта:

$$ROSI > (Nдеп – Nінф)/100), \quad (3.22)$$

де Nдеп – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, 18%;

Nінф – річний рівень інфляції, 13,7%.

$$15 > (18\text{-}13,7)/100$$

$$15 > 0,043$$

Для вибраного варіанта визначається розрахунковий строк окупності капітальних інвестицій $T_o$.

Термін окупності капітальних інвестицій $T_o$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{31636}{489001,4} = 0,065 \approx 24 \text{ дні}.$$

## 3.7 Висновки до економічного розділу

В результаті розрахунку витрат на впровадження програми і методики проведення аналізу рівня захищеності системи «Бітрікс: Управління сайтом» версії 18.х було визначено, що розмір капітальних витрат складатиме 31 636 грн, а щорічні експлуатаційні витрати 206 144,2 грн. Передбачається, що для повної перевірки капітальні витрати становитимуть у 2 рази більше.

Коефіцієнт повернення інвестицій ROSI, при використанні засобів безпеки, які дозволено використовувати завдяки програмі та методиці показав, що становить 15 грн додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження програми і методики.

Загальний ефект використання засобів безпеки, які дозволено використовувати завдяки програмі та методиці, визначається з урахуванням ризиків порушення інформаційної безпеки і становить 489 001,4 грн

Було доведено, що використання засобів безпеки, які дозволено використовувати завдяки програмі та методиці в організації збереже від збитків у розмірі від 1 до 1 737 864 грн грн та  окупиться лише за 24 дні.

# ВИСНОВКИ

У дипломній роботі було розроблено програму та методику, на основі яких був виконаний аналіз рівня захищеності системи «Бітрікс: Управління сайтом» версії 18.х.

Оскільки до переліку засобів ТЗІ дозволених для забезпечення технічного захисту державних інформаційних ресурсів входить система «Бітрікс: Управління сайтом» версії 15.х, а її експертний висновок на разі не є дійсним, то для доказу захищеності системи потрібно робити перевірку самостійно. Для доказу захисту системи «Бітрікс: Управління сайтом» було створено програму та методику проведення аналізу рівня захищеності.

Перевірялися лише ті функціональні послуги безпеки, що могли забезпечуватися елементами модуля «Проактивний захист». Для проведення перевірки цілої системи потрібно перевірити додаткові функціональні послуги безпеки.

Оскільки для забезпечення захисту веб-додатків потрібно знати їх вразливості, було визначено поширені вразливості веб – додатків. Проведено огляд системи «Бітрікс: Управління сайтом» та розглянуто елементи модуля «Проактивний захист».

В економічному розділі наведено обгрунтування запропонованої програми та методики.

Практичне значення роботи полягає зменшення часу та фінансових витрат при проведенні оцінки захищеності та експертизи систем. Результати здійснених у дипломній роботі досліджень можуть бути використані для проведення експертизи систем захисту з використанням системи «Бітрікс: Управління сайтом» версії 18.х.

# ПЕРЕЛІК ПОСИЛАНЬ

1 Веб-приложение Wikipedia [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Веб-приложение

2 Angela Stringfellow «What is Web Application Architecture» [Електронний ресурс]. – Режим доступу: https://stackify.com/web-application-architecture/

3 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу НД ТЗІ 2.5-010-03 [Електронний ресурс]. – Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106344

4 Основные этапы разработки веб приложений [Електронний ресурс]. – Режим доступу: http://akonan.ru/index.php?id=15

5 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу НД ТЗІ 1.1-003-99 [Електронний ресурс]. – Режим доступу: https://tzi.com.ua/downloads/1.1-003-99.pdf

6 Міжнародний стандарт ISO/IEC 29147 [Електронний ресурс]. – Режим доступу: http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip#en

7 Офіційний сайт проекту OWASP Project [Електронний ресурс]. – Режим доступу:https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project

8 Рейтинг вразливостей OWASP Top – 10 – 2017 Електронний ресурс]. – Режим доступу: https://www.owasp.org/images/7/72/OWASP_Top_10-2017_%28en%29.pdf.pdf

9 The Web Application Security Consortium [Електронний ресурс]. – Режим доступу: http://www.webappsec.org

10 Web Application Security Consortium – Класифікація загроз [Електронний ресурс]. – Режим доступу: http://projects.webappsec.org/f/WASC-TC-v2_0.pdf

11 Система керування вмістом [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Система_керування_вмістом

12 Система управления содержимым [Електронний ресурс]. – Режим доступу: https://ru.wikipedia.org/wiki/Система_управления_содержимым#cite_note-_84d2b28cf6796550-3

13 Исследование безопасности CMS-систем 2014 [Електронний ресурс]. – Режим доступу: http://www.ruward.ru/sitesecure/sms-survey/

14 Рейтинг топ cms за 2018 год (промежуточный) [Електронний ресурс]. – Режим доступу: https://it-rating.in.ua/rating-cms-2018-p1

15 Бітрікс: Управління сайтом [Електронний ресурс]. – Режим доступу: https://www.bitrix.ua/products/cms/index.php

16 Редакції продукту Бітрікс [Електронний ресурс]. – Режим доступу: https://www.bitrix.ua/products/cms/editions/#tab-table-link

17 Безпека Бітрікс [Електронний ресурс]. – Режим доступу: https://www.bitrix.ua/products/cms/security/

18 Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу НД ТЗІ 2.5-004-99 [Електронний ресурс]. – Режим доступу: https://tzi.ua/assets/files/НД-ТЗІ-2.5-004-99.pdf

19 Одноразовий пароль [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/Одноразовий_пароль

20 Двухэтапная авторизация [Електронний ресурс]. – Режим доступу: http://prj.23project.top/bitrix/admin/security_otp.php?lang=ru

21 Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [Електронний ресурс]. – Режим доступу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288071&cat_id=44795

22 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-05 [Електронний ресурс]. – Режим доступу: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=46074&cat_id=38835

23 История версий [Електронний ресурс]. – Режим доступу: https://www.1c-bitrix.ru/products/cms/versions.php?module=security

24 PHP [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/PHP

25 1С-Битрикс и PHP 7: ускоряем сайт в 2 раза за 5 минут [Електронний ресурс]. – Режим доступу: https://www.intervolga.ru/blog/support/1c-bitrix-with-php-7/

26 Bitrix и PHP7 - быстрее, выше, сильнее [Електронний ресурс]. – Режим доступу: https://digital-spectr.com/blog/1c-bitrix-php7/

27 Методичні вказівки з оцінювання функціональних послуг безпеки в засобах захисту інформації від несанкціонованого доступу [Електронний ресурс]. – Режим доступу: www.dsszzi.gov.ua/dsszzi/doccatalog/document?id=106347

28 Сайт інтернет магазину [Електронний ресурс]. – Режим доступу: http://prj.23project.top

29 Методичні рекомендації до виконання дипломних робіт (проектів) бакалаврів та магістрів спеціальностей 125 Кібербезпека, 172 Телекомунікації та радіотехніка / Упоряд.: О.Ю. Гусєв, О.В. Герасіна, О.М. Алексєєв,О.В. Кручінін. – Дніпро: НГУ, 2018. – 50 с.

ДОДАТОК А. Відомість матеріалів дипломного проекту

| № | Формат | Найменування | Кількість листів | Примітка |
|---|---|---|---|---|
| 1 | А4 | Реферат | 3 | |
| 2 | А4 | Список умовних скорочень | 2 | |
| 3 | А4 | Зміст | 3 | |
| 4 | А4 | Вступ | 1 | |
| 5 | А4 | 1 Розділ | 25 | |
| 6 | А4 | 2 Розділ | 34 | |
| 7 | А4 | 3 Розділ | 14 | |
| 8 | А4 | Висновки | 1 | |
| 9 | А4 | Перелік посилань | 3 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 1 | |
| 12 | А4 | Додаток В | 2 | |
| 13 | А4 | Додаток Г | 1 | |

# ДОДАТОК Б. Перелік файлів на елетронному носії

1. Магістерська робота Гриб М_О_125м-17-1.docx – Пояснювальна записка
2. Гриб М_О.pptx – Презентація

ДОДАТОК В. Відгук керівника кваліфікаційної роботи

**ВІДГУК**

**на дипломну роботу магістра на тему:**

***«Аналіз ефективності елементів модуля «Проактивний захист» системи «Бітрікс: Управління сайтом» версії 18.х»***

**студента групи 125м–17–1** ***Гриба Михайла Олексійовича***

Мета дипломної роботи – створення умов впровадження засобів захисту при створені веб-додатків.

Тема дипломної роботи безпосередньо пов’язана з об’єктом діяльності фахівця за спеціальністю 125 Кібербезпека – розвиток методик тестування засобів захисту.

Задачі дипломної роботи (аналіз особливостей функціонування та вразливостей веб-додатків, аналіз існуючих систем управління вмістом сайту, розробка програми та методики тестування засобів захисту, проведення тестування та обробка отриманих результатів) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Практичне значення результатів проектування полягає у оптимізації проведення робіт з перевірки засобів захисту на відповідність вимогам нормативних документів.

До недоліків дипломної роботи відносяться:

– пункти методики, щодо реалізації деяких послуг, вимагають додаткових експериментальних перевірок;

– структура викладення програми та методики відрізняється від рекомендованої.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Гриб М.О. виявив себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому дипломна робота виконана у відповідності до вимог, що ставляться до дипломної роботи магістра, заслуговує оцінки “добре”, а Гриб М.О. присвоєння йому кваліфікації професіонала із організації інформаційної безпеки.

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.т.н, проф. _____ В.І. Корнієнко

# ДОДАТОК Г. Відгук керівника економічного розділу

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)