Научная статья
УДК 004.056

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕРНЕТ-МАГАЗИНАХ

Даниил Владиславович Третьяков[1], Евгения Васильевна Анянова[2]
[1, 2] Уральский государственный лесотехнический университет, Екатеринбург, Россия
[1] pietrosian2000@list.ru
[2] anyanovagv@m.usfeu.ru

Аннотация. Анализируются методы защиты информации интернет-магазинов, включая шифрование и системы IDS/IPS. Рассмотрены угрозы, такие как кража данных и DDoS-атаки. Приведены рекомендации для повышения безопасности и надежности онлайн-бизнеса.

Ключевые слова: мониторинг, методы защиты информации, шифрование данных

Для цитирования: Третьяков В. Д., Анянова Е. В. Сравнительный анализ методов защиты информации в интернет-магазинах // Научное творчество молодежи – лесному комплексу России = Scientific creativity of youth to the forest complex of Russia : материалы XXI Всероссийской (национальной) научно-технической конференции студентов и аспирантов. Екатеринбург : УГЛТУ, 2025. С. 1082−1085.

Original article

COMPARATIVE ANALYSIS OF INFORMATION PROTECTION METHODS IN ONLINE STORES

Daniil V. Tretyakov[1], Evgeniya V. Anyanova[2]
[1, 2] Ural State Forest Engineering University, Ekaterinburg, Russia
[1] pietrosian2000@list.ru
[2] anyanovagv@m.usfeu.ru

Abstract. The article analyzes methods of protecting information of online stores, including encryption and IDS/IPS systems. Threats such as data theft and DDoS attacks are considered. Recommendations for improving the security and reliability of online business are given.

Keywords: monitoring, methods of information protection, data encryption

For citation: Tretyakov D. V., Anyanova E. V. (2025) Sravnitelnyi analiz metodov zashchity informatsii v internet-magazinakh [Comparative analysis of information protection methods for information system of online stores]. Nauchnoe tvorchestvo molodezhi – lesnomu kompleksu Rossii [Scientific creativity of youth to the forest complex of Russia] : proceedings of the XXI All-Russian (national) Scientific and Technical Conference of undergraduate and postgraduate students. Ekaterinburg : USFEU, 2025. Pp. 1082–1085. (In Russ).

В настоящее время деревообрабатывающая промышленность столкнулась с проблемой защиты информации и рисками информационной безопасности, так как постоянно усовершенствуются методы интернет-мошенничества, увеличивается количество кибератак. Деревообрабатывающая промышленность является одной из развивающихся отраслей экономики. Наблюдается массовая продажа пиломатериала с помощью интернет ресурсов, в частности, через интернет-магазины.

Цель данной статьи – провести сравнительный анализ методов защиты информации, используемых в интернет-магазинах, осуществляющих продажу пиломатериалов, и оценить их эффективность в борьбе с актуальными угрозами.

В задачи входит анализ основных угроз безопасности, характерных для интернет-магазинов, а так же ознакомление с существующими методами и средствами защиты информации и сравнение их по эффективности, стоимости внедрения и сложности эксплуатации. Последним пунктом будет разработка рекомендации по выбору оптимальных подходов для обеспечения информационной безопасности.

Объект исследования: информационные системы интернет-ресурсов.

Предмет исследования: методы и средства защиты информации, используемые для предотвращения угроз и минимизации рисков.

Интернет-магазины являются привлекательной целью для злоумышленников из-за большого объема персональных и финансовых данных, которые они обрабатывают. Хакеры используют широкий спектр методов для нарушения работы систем, кражи данных или вымогательства.

Для начала стоит рассмотреть основные типы угроз на пример атаки через уязвимости на стороне клиента (XSS-атаки). Использование вредоносных скриптов (Magecart) для кражи платежной информации. Массовое увеличение нагрузки на сервер интернет-магазина с целью вывести его из строя (DDoS-атаки). Компрометация учетной записи администратора магазина и так далее.

Во избежание возможных угроз нужно ознакомиться с методами защиты информации.

Первым из таких методов является криптографический метод. Его основной целью считается преобразование математическими методами секретного сообщения, передаваемого по каналам связи, телефонного разговора или компьютерных данных так, что они становятся абсолютно

неясными для сторонних лиц [1]. В случае с интернет-магазином криптографический метод используется для защиты конфиденциальной информации.

Вторым методом является многофакторная аутентификация и управление доступом. Цель многофакторной аутентификации направлена на предотвращение несанкционированного доступа к информационным ресурсам, в нее входят два или более факторов проверки, в основном это пароль и одноразовый код. Ролевое управление доступом разграничивает возможности в зависимости от роли пользователей (администратор и заказчик).

Третий метод – это метод обнаружения и предотвращения атак (IDS/IPS). Системы обнаружения вторжений (IDS) такие как Snort, Suricata анализируют трафик сети для выявления подозрительной активности. Системы предотвращения вторжений (IPS) (CiscoFirepoweri PaloAltoNetworks) блокируют вредоносные действия в режиме реального времени.

Четвертый метод – мониторинг и аудит безопасности. Сбор и анализ данных в программах Splunk, Graylog поспособствуют в выявлении подозрительных действий. Проведение аудита безопасности укажет на существующие уязвимости в информационной системе. Один из способов – тестирование на проникновение (pentest).

Один из важнейших методов – это минимизация человеческого фактора и обучение персонала. Не секрет, что человек ошибается чаще, чем машина, поэтому, чтобы предотвратить всевозможные проблемы, необходимо проводить инструктаж сотрудников по безопасности работы с системами и установить строгие правила, минимализирующие человеческий фактор, например ежемесячная смена паролей и тому подобное.

Для сравнительного анализа методов защиты потребуются критерии, которые смогут отобразить лучшие и худшие стороны каждого из методов: применимость, эффектность, сложность внедрения и стоимость (таблица).

Сравнения методов защиты информации

Метод защиты	Применимость	Эффектность	Сложность внедрения	Стоимость
Шифрование данных	Подходит для всех бизнесов	Высокая	Средняя	Средняя
Многофакторная аутентификация	Подходит для всех бизнесов	–″–	–″–	Низкая
IDS/IPS	Рекомендуется для среднего и крупного бизнеса	–″–	Высокая	Высокая
Мониторинг и аудит безопасности	Подходит для всех бизнесов	–″–	–″–	–″–
Обучение персонала	Подходит для всех бизнесов	Средняя	Низкая	Низкая

Проведя сравнительный анализ, можно сделать выводы, что важно соблюдать комплексный подход, ведь самостоятельное использование одного метода очевидно недостаточно. Эффективность возрастает при комбинировании методов, например шифрование данных в сочетании с многофакторной аутентификацией и регулярным аудитом безопасности. Так же не стоит забывать о человеческом факторе, так как все эти методы могут утерять свою силу без должного обучения персонала, которое является значимым и дешевым элементом защиты информации.

Таким оюразом, можно сформировать рекомендации – выбор оптимальной комбинации методов. Каждый метод вносит разный аспект в информационную безопасность, и выбор зависит только от самого интернет-бизнеса. Так же стоит отметить, что обучение сотрудников основам безопасности является неотъемлемой частью повышения защиты информации, так как сотрудники более уязвимы кибератаками. Последней рекомендацией будет поддержка актуальности ПО, используемого интернет-магазином.

Список источников

1. Назарова А. П. Криптографические методы защиты информации. URL: https://cyberleninka.ru/article/n/kriptograficheskie-metody-zaschity-informatsii/viewer (дата обращения: 29.11.2024).

2. Оладько В. С. Угрозы информационной безопасности в системах электронной коммерции. URL: https://cyberleninka.ru/article/n/ugrozy-informatsionnoy-bezopasnosti-v-sistemah-elektronnoy-kommertsii (дата обращения: 29.11.2024).

3. Интернет-угрозы и способы защиты от них / Д. В. Мазаев, В. В. Ермолаева, А. Г. Мурзагалиев // Молодой ученый. 2015. № 11 (91). С. 193–197. URL: https://moluch.ru/archive/91/19771/ (дата обращения: 29.11.2024).