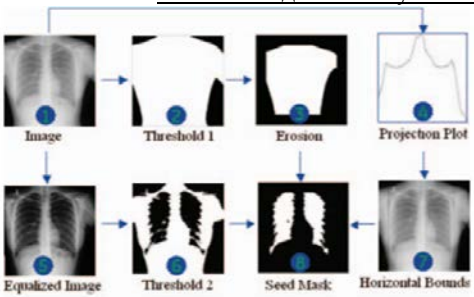

Рисунок 3 - Метод активного контура

Дальнейшая цель — это реализация одного или нескольких алгоритмов и сравнение их эффективности или переход на изучение и выделения признаков конкретной патологии.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Brown, M. S., Wilson, L. S., Doust, B. D., Gill, R. W., & Sun, C. Knowledge-based method for segmentation and analysis of lung boundaries in chest X-ray images. [Текст] // Computerized Medical Imaging and Graphics.-1998.-Vol.22(6). –P.463–477.

2. Annangi, P., Thiruvenkadam, S., Raja, A., Xu, H., Sun, X., & Mao, L. A region based active contour method for x-ray lung segmentation using prior shape and lowlevel features. [Текст] // IEEE International Symposium on Biomedical Imaging: From Nano to Macro. –2010 .

3. Ильясова, Н.Ю. Информационные технологии анализа изображений в задачах медицинской диагностики [Текст]/ Н.Ю.Ильясова, А.В.Куприянов, А.Г.Храмов. – М.:Радио и связь. – 2012. – 424 с.

УДК 004.056.53

РАЗРАБОТКА ОБУЧАЮЩЕЙ СИСТЕМЫ ПО ОСНОВАМ ВЕБ-БЕЗОПАСНОСТИ

Ф. А. Дмитриев[1]

Научный руководитель: Е. В. Мясников, к.т.н., доцент

Ключевые слова: информационная безопасность, уязвимость, веб-безопасность, несанкционированный доступ, защита веб-сайта,

Множество современных общедоступных интернет-ресурсов содержат уязвимости, которые могут использоваться

[1] Федор Александрович Дмитриев, студент группы 6311-100503D, email: fedor0299@rambler.ru

злоумышленниками для извлечения выгоды. Из этого следует необходимость обеспечения этих ресурсов соответствующим уровнем защиты. На рынке информационных услуг существует большой спрос на проектирование сайтов различной сложности. Зачастую заказчики даже не знают о том, что их сайт будет иметь дело с конфиденциальной информацией и должен быть обеспечен необходимым уровнем защиты. Поэтому пользуются услугами низкооплачиваемых специалистов с низкой компетентностью в области web-безопасности.

Низкий спрос на проектирование безопасных интернет-ресурсов является не единственной причиной отсутствия защиты пользовательских данных. Существует явный дефицит обучающего материала о web-безопасности для начинающих разработчиков.

Актуальность данной работы заключается в том, что она поможет решить проблему низкой защищенности интернет-ресурсов, предоставляя обучающий материал в игровой форме, понятный даже новичкам.

Целью работы стала разработка онлайн-системы для обучения веб-разработчиков основам web-безопасности для повышения безопасности сайтов и предотвращения несанкционированного доступа.

В качестве базовой системы были взяты существующие англоязычные системы, обучающий информационной безопасности. Были разработаны оптимальные требования к обучающим системам. Проанализированы 15 существующих системы (bWAPP, HackThis!, OWASP Mutillidae II, HackThisSite, Google Gruyere, DVIA, Hellbound Hackers, WebGoat, Root Me, OverTheWire) на соответствие заданным требованиям. В этих системах не выполняется требование по доступности контента для русскоязычного сегмента, и они ориентированы в основном на старшую возрастную категорию. Поэтому для устранения этих недостатков выбран путь разработки собственной системы.

Отличительной чертой разработанной системы является доступность на русскоязычном сегменте и возможность изучения уязвимостей и их последствий на практике. Основной акцент в разработке был сделан на такие уязвимости как XSS (Cross-Site Scripting) Injections и SQL Injections.

В дальнейшим планируется модернизировать систему, которая сможет работать не только в онлайн режиме, но и в локальном для того, чтобы увеличить функциональность приложения. Сделать акцент не только на веб-безопасность, но и на информационную безопасность в целом. Например, добавление задач по CTF (Capture the flag).