УДК 004.056

Оладько Владлена Сергеевна
к.т.н., доцент
Волгоградский государственный университет
г. Волгоград, Российская Федерация
Микова Софья Юрьевна
студент 4 курса
Волгоградский государственный университет
г. Волгоград, Российская Федерация
Нестеренко Максим Алексеевич
студент 4 курса
Волгоградский государственный университет
г. Волгоград, Российская Федерация

Oladko V. S.
Ph.D., Associate Professor, Volgograd State University
Volgograd, Russian Federation
Mikova S. Y.
4th year student, Volgograd State University
Volgograd, Russian Federation
Nesterenko M. A.
4th year student, Volgograd State University
Volgograd, Russian Federation

ТЕХНОЛОГИИ ЗАЩИТЫ ИНТЕРНЕТ-ТЕХНОЛОГИЙ И WEB-ПРИЛОЖЕНИЙ

THE PROTECTION TECHNOLOGY FOR INTERNET TECHNOLOGIES AND WEB-APPLICATIONS

Аннотация. *Исследована проблема нарушения безопасности интернет-технологий. Описана типовая архитектура web-приложения. Разработана классификация угроз web-приложений и описаны их последствия. Обозначены направления и технологии защиты. Представлен жизненный цикл процесса создания и сопровождения защищенного web-приложения.*

Ключевые слова: *информационная безопасность, интернет, статистика угроз безопасности, система защиты, электронная коммерция, межсетевой экран уровня приложения, защита соединения.*

Summary. *The problem of security breaches of Internet technologies studied.*

Typical architecture of web-applications is described. Classification of threats of web-applications developed. The consequences of threats and attacks described. The authors were identified direction and protection technology. The life cycle of the process of creating and support a protected web-applications is described.

Keywords: *information security, internet, statistics security threats, system protection, e-commerce, WAF, secure connection.*

На сегодняшний день в мире большое развитие и распространение получили различные интернет-технологий, которые используются в самых различных отраслях деятельности: электронная коммерция, порталы государственных и бытовых услуг, форумы и чаты, социальные сети, новостные и аналитические порталы, электронная почта, теле — видео конференции, персональные web-сайты и блоги. Для реализации перечисленных систем используются web-приложения, представляющие собой клиент-серверные приложения, в которых клиентами являются браузеры пользователей, а сервером — web-сервер.

Логика веб-приложения распределена между сервером и клиентом, хранение данных осуществляется, преимущественно, на сервере, обмен информацией происходит по сети. Само web-приложение может выступать в качестве клиента других служб, например, базы данных или другого web-приложения, расположенного на другом сервере. Большинство web-приложений являются распределёнными, и в общем виде их типовую архитектуру (см. рис. 1), можно представить в виде четырех взаимодействующих уровней: клиент (web-браузер, отправляющий запрос), web-сервер, бизнес-логика (приложение), данные (БД, статика).

В зависимости от области применения web-приложения в нем может обрабатываться информация различного уровня доступа и ценности, например платежные и персональные данные пользователей, информация о банковских картах и счетах, идентификационные данные и пароли. Данная информация в процессе своей обработки, передачи и хранения может быть подвержена ряду воздействий случайного и злоумышленного характера. Причем наибольше число негативных воздействий, по данным [1, с. 17], приходиться на электронную коммерцию (30%), финансовый и банковский сектор (22%), промышленность (17%) и информационную инфраструктуру и технологии (15%). Основными предпосылками для реализации подобных воздействий, по данным [1, с. 20], являются: недостатки реализации системы защиты web-приложения; уязвимости в коде приложения (36%); недостатки и ошибки конфигурации (22%).

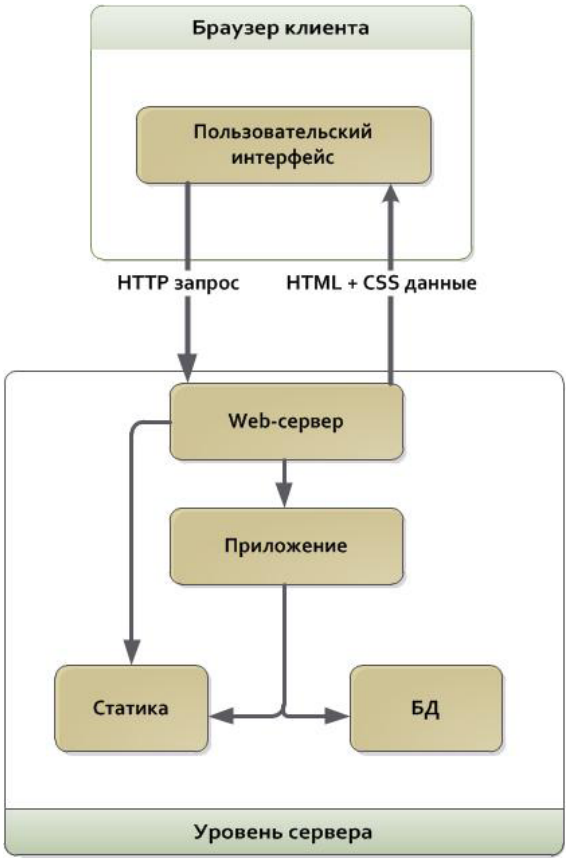

Рис. 1. Архитектура web -приложения

На основании анализа типовой архитектуры web-приложения и аналитики по нарушениям информационной безопасности за 2014–2015 годы [1–4],

Таблица 1

Классификация угроз безопасности web-приложениям

№	Группа угроз	Примеры угроз	Последствия от угроз
1	Угрозы, связанные с эксплуатацией уязвимостей в коде web-приложения	SQL-инъекции XSS-атаки PHP-инъекции Подделка межсайтовых запросов — CSRF	Получение несанкционированного доступа к файлам и БД web-приложения, нарушение конфиденциальности и целостности информации
2	Сетевые атаки	Атаки на браузер клиента web-приложения Перебор паролей и атаки на систему аутентификации пользователей Отказ в обслуживании сервисов web-приложений Сканирование сети Вызов исключительных ситуаций	Получение несанкционированного доступа к файлам и БД web-приложения, получение доступа к компьютеру пользователя, нарушение доступности, конфиденциальности и целостности информации
3	Угрозы случайного характера	Сбои и отказы программно-аппаратных средств Стихийные бедствия	Нарушение доступности информации и сервисов web-приложения, финансовые потери
4	Мошенничество	Спам — рассылки Фишинг Отказ от обязательств и совершенных действий Нарушение авторского права	Финансовые и репетиционные потери

*Составлено авторами на основании [1–4]

авторами была разработана классификация угроз для web-приложений, представленная в таблице 1.

Наиболее распространёнными атаками на web-приложения стали сетевые атаки (см. рис. 2.), направленные на: браузер клиентов web-приложения (26%), отказ в обслуживании сервисов web-приложений (22%), на систему аутентификации пользователей (18%). При этом большинство атак было реализовано с помощью вредоносного программного обеспечения, только веб — антивирусом Касперского было детектировано 28 483 783 уникальных вредоносных объектов: скриптов, эксплойтов, исполняемых файлов и т.д.

В результате успешной реализации угроз происходит нарушение доступности, целостности и конфиденциальности информации, при этом наибольший интерес для злоумышленника представляю персональные и платежные данные пользователей, на которые, по данным [2], приходится около 90% утечек. В результате пострадавшая сторона несет финансовые и репутационные потери.

Для предотвращения атак и снижения рисков от возможных угроз необходимо применять специальные технологии и средства защиты web-приложений. Анализ [5–9] показывает, что обеспечение защиты должно осуществляться как на этапе проектирования и разработки самого web-приложения, путем создания безопасного кода web-приложения и планирования рационального состава системы защиты, так и в процессе его эксплуатации с внесением в случае необходимости своевременных корректировок. Поскольку даже если web-приложение написано без ошибок и уязвимости в нем нет, необходима комплексная защита, учитывающая наличие базы данных приложений, веб-сервера и прочих элементов ИТ-платформы. Исходя из этого, защиту предлагается строить по следующим направлениям:

– контроль за безопасностью кода web-приложения на протяжение всего жизненного цикла разработки;
– обеспечение защиты информации во время её передачи между компьютером клиента и web-сервером;
– обеспечение защиты информации сохраняемой на компьютере клиента;
– использование специализированных средств защиты информации на уровне web-сервера.

Это достигается за счет применения следующих средств и методов защиты:

– недопущение ошибок в скриптах при разработке web-приложения;
– сканирование кода web-приложения на наличие уязвимостей и установка специальных водяных знаков (например с помощью Trend Micro Deep Security).
– использование систем многофакторной аутентификации пользователей (например, парольная аутентификация с секретным кодом, E-num, сертификаты, цифровые подписи, биометрическая аутентификация);
– применение антивирусного программного обеспечения;
– применение защищенных каналов связи и сетевых протоколов при установке соединения клиента

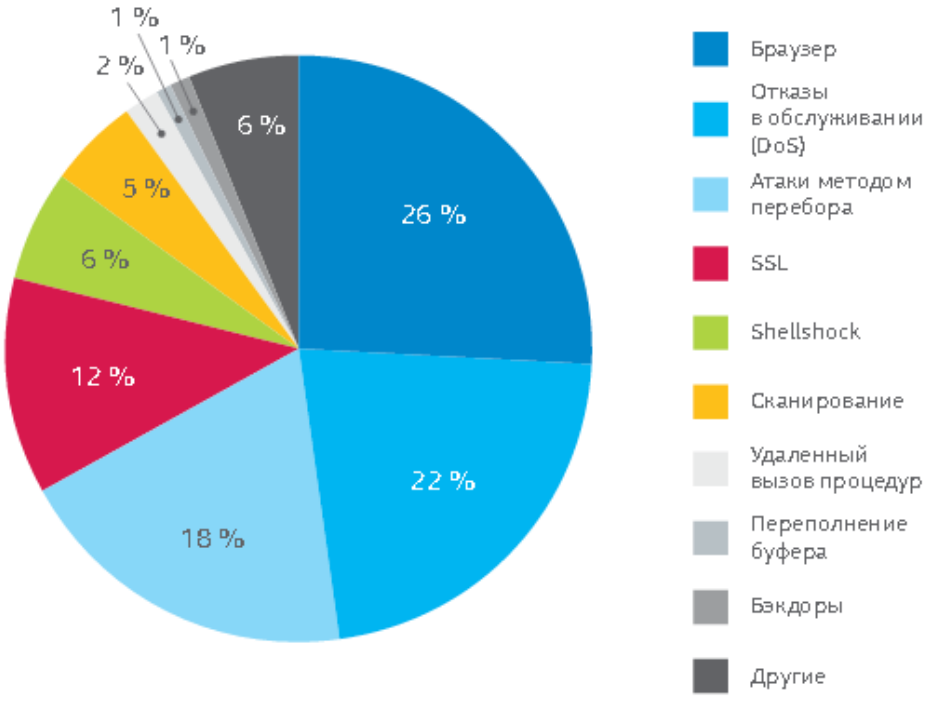

Рис. 2. Статистика сетевых атак на web-приложения за 2015 год, по данным McAfee Labs [4, с. 45]

с web-сервером и передачи данных между ними (например, VPN, HTTPS);
- использование обратных прокси-серверов и прикладных шлюзов (пример mod_security для Apache) на уровне web-сервера;
- применение локальных и сетевых систем обнаружения вторжений;
- применение специализированных межсетевых экранов уровня приложений (например, решения типа ApplicationFirewall, IMPERVA Web Application Firewall, Fortigate Web, Barracuda WAF, CheckPoint Web Security Blade), которые обладают встроенным функционалом предотвращения вторжений и обеспечивают защиту от целенаправленных web-атак, таких как переполнение буфера, SQL инъекции, Cross-Site-Scripting, изменение параметров запросов и других. Решения этого класса фильтруют запросы на доступ к приложению и блокируют все действия, которые не относятся к разрешенной активности пользователей.

Все эти меры требуется выполнять в комплексе, поскольку защита по раздельности не принесет желаемого эффекта. Таким образом, жизненный цикл разработки и сопровождения защищенного web-приложения предлагается реализовывать в виде циклического процесса (см. рис. 3). Это решение обусловлено тем, что угрозы, как в отношении определенного направления использования web-приложения, так и конкретных технологий меняются очень быстро, поэтому важно регулярно отслеживать статистику угроз интернет-технологиям, анализировать выявленные инциденты безопасности и оценивать риски их влияния на систему защиты web-приложения.

Процесс многократно начинается с определения бизнес-требований к web-приложению, определяющих стоящие перед ним задачи и его функциональные возможности. При этом большую роль играет этап сбора информации и принятия решений. Технически непосредственная разработка защищенного web-приложения начинается только на последнем этапе (прямоугольник «Реализация служб защиты, выбор средств защиты»). Это связано с тем, что такой объем исследовательской работы и планирования помогает убедиться в том, что окончательное решение по обеспечению защиты наилучшим образом соответствует требованиям к уровню безопасности и позволяет привести потенциальные риски от угроз к допустимым.

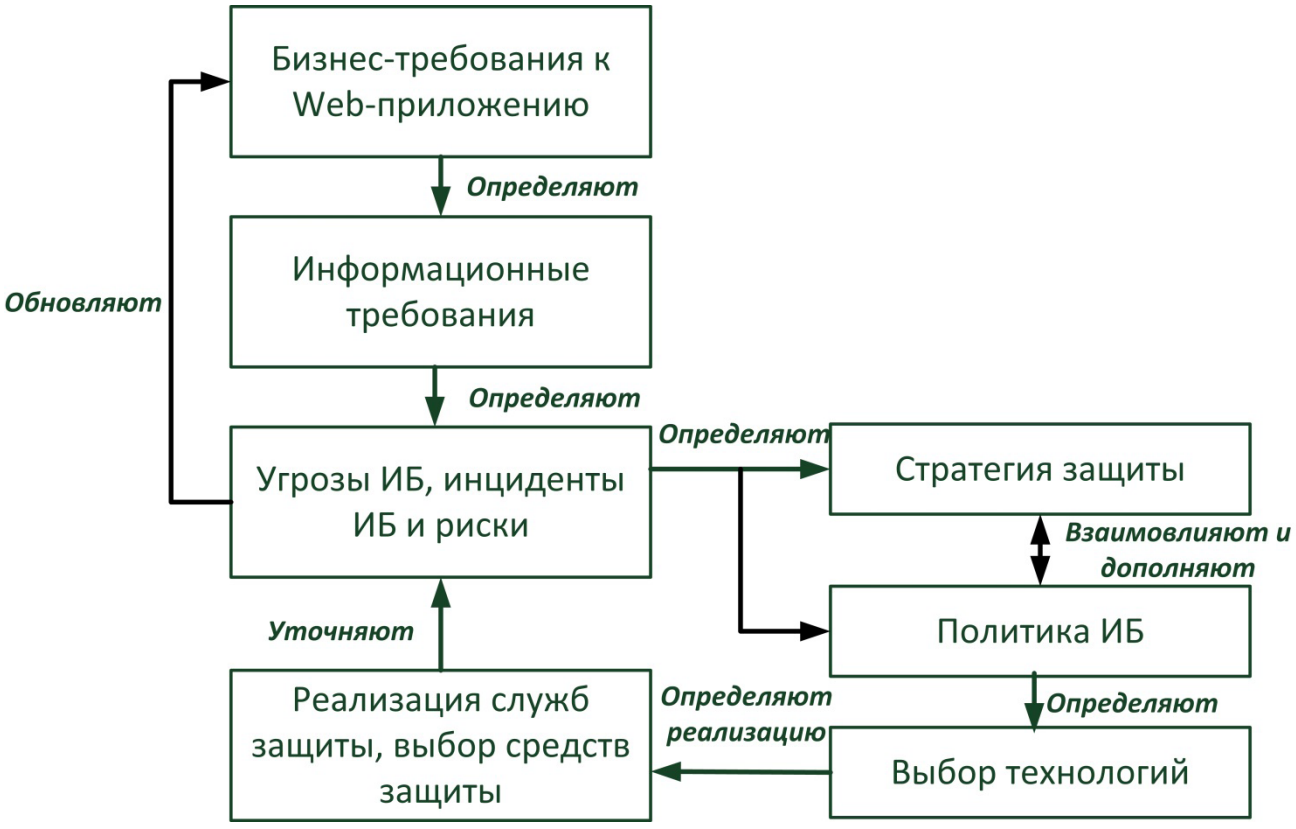

Рис. 3. Жизненный цикл разработки и сопровождения защищенного web-приложения (разработано авторами)

Литература

1. Сборник исследований по практике безопасности [Электронный ресурс //Positive Technologies. 2015]. URL: http://www.ptsecurity.ru/download/PT_Positive_Research_2015_RU_web.pdf (дата обращения 18.11.2015)

2. Глобальное исследование утечек конфиденциальной информации в I полугодии 2015 года [Электронный ресурс]. // Аналитический центр InfoWatch. URL: http://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2015_half_year.pdf (дата обращения 18.11.2015).

3. Гарнаева М., Чебышев В., Макрушин Д., Иванов А. Развитие информационных угроз в первом квартале 2015 года [Электронный ресурс] //Квартальные отчеты об угрозах SECURELIST. URL: https://securelist.ru/analysis/malware-quarterly/25544/razvitie-informacionnyx-ugroz-v-pervom-kvartale-2015-goda/ (дата обращения 18.11.2015).

4. Отчет McAfee Labs об угрозах за февраль 2015 [Электронный ресурс] //Компания McAfee Labs. URL: http://www.mcafee.com/ru/resources/reports/rp-quarterly-threat-q4-2014.pdf?cid=BHP035 (дата обращения 18.11.2015).

5. Оладько В. С. Механизмы защиты web-приложений от внедрения вредоносного кода// Новый университет. Серия: Технические науки. 2015. № 3–4 (37–38). С. 64–68.

6. Дорогов П. Современные вызовы и риски при использовании информационных технологий для управления бизнесом [Электронный ресурс]//Балтийский курс. Вызовы и аналитика. URL: http://www.baltic-course.com/rus/kruglij_stol/?doc=40218 (дата обращения 18.11.2015).

7. Кузнецов И. А., Оладько В. С., Микова С. Ю., Нестеренко М. А. Методы обеспечения информационной безопасности в социальных сетях// Актуальные вопросы науки. 2015. № XIX. — С. 10–14.

8. Бабенко А. А., Безбабнов Д. В., Витенбург Е. А.. Исследование систем управления информационным наполнением web-ресурсов // Актуальные вопросы информационной безопасности регионов в условиях глобализации информационного пространства: материалы IV Всерос. науч.-практ. конф., г. Волгоград, 23–24 апр. 2015 г.; Федер. гос. авт. образоват. учреждение высш. проф. образования «Волгогр. гос. ун-т» — Волгоград: Изд-во ВолГУ, 2015 — С. 92–96.

9. Оладько А. Ю., Аткина В. С. Модель защиты интернет-магазина//Известия ЮФУ. Технические науки. 2014. № 2 (151). С. 74–80.