POSITIVE TECHNOLOGIES

СТАТИСТИКА УЯЗВИМОСТЕЙ ВЕБ-ПРИЛОЖЕНИЙ ЗА 2010-2011 ГОДЫ

Сергей Гордейчик
Дмитрий Евтеев
Александр Зайцев
Денис Баранов
Сергей Щербель
Анна Белимова
Глеб Грицай
Юрий Гольцев
Тимур Юнусов
Илья Крупенко
Иван Полиянчук
Сергей Бобров
Сергей Дроздов
Владимир Кочетков
Юрий Дьяченко
Андрей Медов
Дмитрий Серебрянников
Артем Чайкин

МОСКВА
2012

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Многолетний опыт компании Positive Technologies по проведению тестов на проникновение и аудита информационной безопасности, а также экспертиза исследовательского центра Positive Research, показывают, что ошибки в защите веб-приложений по-прежнему остаются одним из основных недостатков обеспечения защиты информации. Более того, уязвимости веб-приложений являются одним из наиболее распространенных путей проникновения в корпоративные информационные системы; существует множество факторов, делающих веб-сервисы привлекательной целью для атак злоумышленников.

Усилия разработчиков приложений обычно направлены главным образом на решение задач, связанных с реализацией функций системы. Вопросам безопасности и качества программного кода уделяется недостаточно внимания. В результате подавляющее большинство веб-приложений содержит уязвимости различной степени критичности.

Простота протокола HTTP позволяет разрабатывать эффективные методы автоматического анализа веб-приложений и выявления в них уязвимостей. Это значительно упрощает работу нарушителя, позволяя ему обнаружить большое число уязвимых веб-сайтов, чтобы затем провести атаку на те, которые представляют наибольший интерес.

Кроме того, уязвимости некоторых типов допускают не только автоматическое выявление, но и автоматическую эксплуатацию. Именно таким образом производится массовое внедрение в веб-ресурсы вредоносного кода, который затем используется для создания ботнетов из рабочих станций обычных пользователей сети Интернет. Возможность использования веб-приложений в качестве платформы для атаки на рабочие места пользователей сама по себе делает эти приложения привлекательной целью для нарушителя.

Таким образом, при подготовке атаки на информационную инфраструктуру компании злоумышленники в первую очередь исследуют ее веб-приложения. Недооценка риска, который могут представлять уязвимости в веб-приложениях, доступные из сети Интернет, является, возможно, основной причиной низкого уровня защищенности большинства из них.

2. МЕТОДИКА ИССЛЕДОВАНИЯ

Данная публикация содержит обзорную статистику уязвимостей веб-приложений, полученную в ходе тестирования на проникновение, аудита безопасности и других работ, выполненных экспертами компании Positive Technologies в 2010 и 2011 годах. Были собраны данные по детальному тестированию 123 сайтов, в которых было обнаружено 1817 уязвимостей различной степени риска. Оценка защищенности проводилась ручным способом по методам черного и белого ящиков с использованием вспомогательных автоматизированных средств. Метод черного ящика заключается в проведении работ по оценке защищенности информационной системы без предварительного получения какой-либо информации о ней со стороны владельца. Метод белого ящика заключается в том, что для оценки защищенности информационной системы используются все необходимые данные о ней, включая исходный код приложений. В статистику вошли данные только по внешним веб-приложениям, доступным из глобальной сети Интернет.

Обнаруженные уязвимости классифицировались согласно системе Web Application Security Consortium Threat Classification (WASC TC v. 2 [1]), за исключением уязвимостей Improper Input Handling, Improper Output Handling и Denial of Service, поскольку они реализуются при эксплуатации множества других уязвимостей. Проект WASC TC представляет собой попытку классифицировать все угрозы безопасности веб-приложений. Члены Web Application Security Consortium создали его для разработки и популяризации стандартной терминологии описания проблем безопасности веб-приложений. Этот документ дает возможность разработчикам приложений, специалистам в области безопасности, производителям программных продуктов и аудиторам использовать для взаимодействия единый язык. В разработке системы Threat Classification активное участие принимали эксперты компании Positive Technologies.

В приводимой статистике учитываются только уязвимости веб-приложений. Другие распространенные проблемы информационной безопасности (к примеру, недостатки процесса управления обновлениями программного обеспечения) не рассматриваются.

Степень критичности уязвимости оценивалась согласно системе Common Vulnerability Scoring System (CVSS v. 2 [2]), выделялись высокий, средний и низкий уровень риска.

3. РЕЗЮМЕ

В данном разделе приведены наиболее значимые заключения по статистическому анализу уязвимостей, выявленных в 123 веб-приложениях в ходе тестирований, проведенных в 2010 и 2011 годах компанией Positive Technologies.

1. Все исследованные сайты содержали уязвимости, причем **64% сайтов — уязвимости высокого уровня риска**, 98% — среднего, и 37% — низкого.

2. По результатам тестирований за два года сформирован топ-10 самых часто встречаемых уязвимостей веб-ресурсов. Первое место в списке занимает Cross-Site Request Forgery (CSRF), которой был подвержен 61% исследованных ресурсов. **В топ вошли три критические уязвимости — SQL Injection, OS Commanding и Path Traversal** с результатами в 47%, 28% и 28% сайтов соответственно.

3. Исследование поквартальной динамики показало, что количество сайтов с уязвимостями высокого и низкого уровня риска сократилось в 2011 году по сравнению с 2010 годом. В частности это касается одной из наиболее распространенных уязвимостей — SQL Injection. При этом доля сайтов, на которых выявлена самая распространенная уязвимость — Cross-Site Request Forgery, — напротив, выросла в 2011 году.

4. PHP оказался самым популярным языком программирования веб-приложений — на нем написано 63% протестированных ресурсов — и вместе с тем самым незащищенным. Сравнение защищенности сайтов на языках PHP, ASP.NET и Java проводилось по уязвимостям, обусловленным ошибками в программной реализации. **Исследование показало, что 81% сайтов на PHP содержат критические уязвимости такого рода,** 91% — уязвимости средней степени риска. Наименее распространены критические уязвимости среди сайтов, написанных на ASP.NET: только 26% из них содержат уязвимости высокого уровня риска; это значительно меньше, чем у PHP (81%) и Java (59%).

5. Веб-сервер nginx продемонстрировал наибольшую склонность к наличию уязвимостей, связанных с ошибками администрирования, значительно превзойдя по их распространенности сервера Apache и Microsoft IIS.

6. При анализе защищенности веб-ресурсов, принадлежащих к различным отраслям экономики, относительно низкая доля сайтов, содержащих критические уязвимости, была выявлена в финансовом секторе. **Лидером по количеству уязвимых сайтов оказался телекоммуникационный сектор.**

7. Сайты на основе систем управления содержимым (Content Management System, CMS) собственной разработки значительно более уязвимы, чем те, которые используют коммерческие или свободные CMS. При сравнении коммерческих и свободных систем большую защищенность демонстрируют первые (за исключением показателей по отдельным уязвимостям). Ресурсы со свободными системами значительно чаще остальных оказываются заражены вредоносным кодом.

8. Для веб-приложений, на которых обнаружен вредоносный код, характерно широкое распространение уязвимостей OS Commanding и Improper Filesystem Permissions.

9. Отдельный анализ систем дистанционного банковского обслуживания (ДБО) обнаружил, что в них практически не встречаются критические уязвимости, в том числе и распространенная уязвимость SQL Injection. **Доля уязвимостей с высоким уровнем риска на сайтах ДБО значительно меньше среднего показателя по всем системам.**

10. Проверка соответствия веб-приложений финансового сектора требованиям стандарта безопасности платежных карт Payment Card Industry Data Security Standard (PCI DSS) показала, что **лишь 10% исследованных приложений удовлетворяют стандарту**.

4. ПОРТРЕТ УЧАСТНИКОВ

Статистическое исследование опирается на данные, полученные в результате проведения подробного анализа защищенности 123 веб-приложений. С точки зрения отраслевой принадлежности были выделены следующие группы владельцев сайтов: информационные технологии, государственный и финансовый секторы, телекоммуникации, промышленность. Небольшое количество представителей образования, строительства, энергетики не позволило сформировать достаточно точные статистические данные, поэтому соответствующие ресурсы были объединены в группу «Другие». Наиболее широко представлены государственный сектор (25%) и сайты телекоммуникационных компаний (26%). Однако они не имеют преобладающего преимущества, остальные секторы также составляют значительные доли в исследуемой выборке (см. табл. 1 и рис. 1).

Таблица 1. Распределение участников по отраслям экономики

Отрасль экономики	**Доля, %**
Телекоммуникации	26
Государственный сектор	25
Финансовый сектор	17
Информационные технологии	13
Промышленность	7
Другие	12

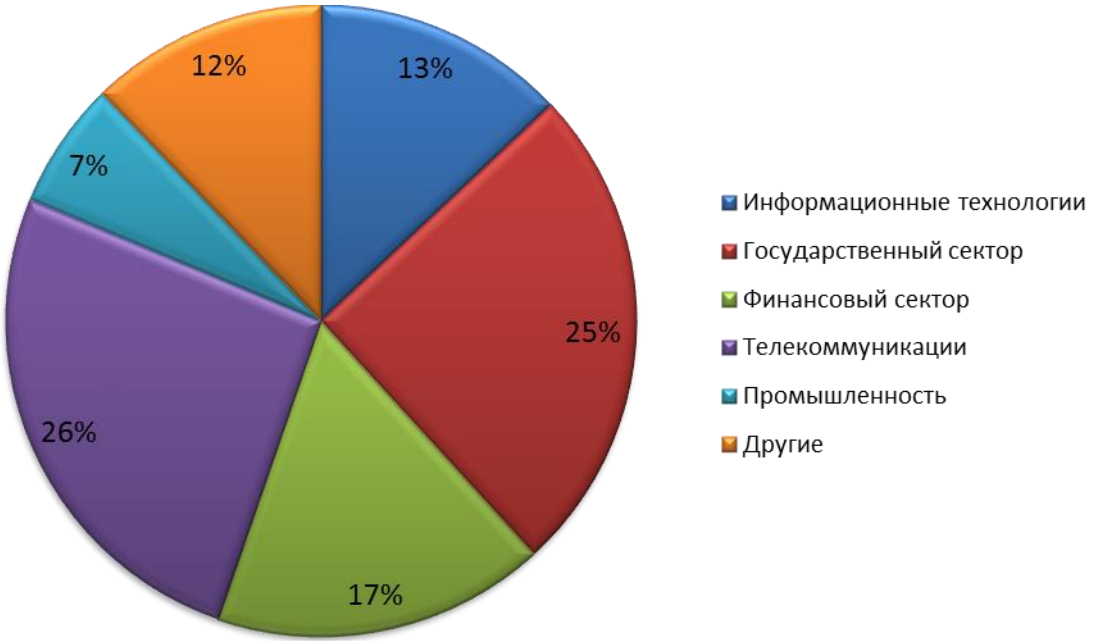

Рисунок 1. Распределение участников по отраслям экономики

5. СТАТИСТИКА УЯЗВИМОСТЕЙ

Данная глава содержит анализ распространенности и уровней критичности уязвимостей различных типов, классифицированных согласно WASC TC v. 2. В разделе 5.1 представлен топ-10 наиболее распространенных в эти годы уязвимостей. В разделе 5.2 приведена динамика наличия уязвимостей на сайтах с опорой на поквартальные данные за 2010 и 2011 годы. В разделе 5.3 проводится сравнительный анализ наличия уязвимостей на сайтах, написанных на различных языках программирования. В разделе 5.4 — анализ уязвимостей на сайтах, работающих под управлением различных веб-серверов. Раздел 5.5 посвящен сравнению уязвимостей, характерных для различных областей экономики. В разделе 5.6 сопоставляется подверженность атакам ресурсов с системами управления содержимыми собственной разработки, коммерческими и свободными. Раздел 5.7 содержит анализ уязвимостей, которые были обнаружены на сайтах, зараженных вредоносным кодом. В разделе 5.8 проводится исследование уязвимостей в системах дистанционного банковского обслуживания. В разделе 5.9 приведен анализ соответствия сайтов — участников тестирования из финансового сектора требованиям стандарта PCI DSS, связанным с безопасностью веб-приложений.

5.1. ТОП-10 НАИБОЛЕЕ РАСПРОСТРАНЕННЫХ УЯЗВИМОСТЕЙ

По результатам анализа защищенности все исследованные ресурсы содержали хотя бы одну уязвимость. Десять уязвимостей, выявленных на наибольшем количестве сайтов, представлены на рис. 2. Лидер в этом списке — Cross-Site Request Forgery, которой оказался подвержен 61% всех проверенных сайтов. Далее следуют Information Leakage и Brute Force — 54% и 52% сайтов, а также SQL Injection с критическим уровнем риска, обнаруженная на 47% ресурсов. На более низких позициях в список входят еще две уязвимости с высокой степенью риска — OS Commanding и Path Traversal (обе с долей уязвимых сайтов в 28%). В список десяти самых распространенных уязвимостей вошли также недостатки среднего уровня риска: Insufficient Anti-automation (42% исследованных сайтов), Cross-Site Scripting (40%), Predictable Resource Location (36%) и Insufficient Transport Layer Protection (22%).

Таблица 2. Наиболее распространенные уязвимости

Уязвимость	**Доля сайтов, %**
Cross-Site Request Forgery	61
Information Leakage	54
Brute Force	52
SQL Injection	47
Insufficient Anti-automation	42
Cross-Site Scripting	40
Predictable Resource Location	36
OS Commanding	28
Path Traversal	28
Insufficient Transport Layer Protection	22

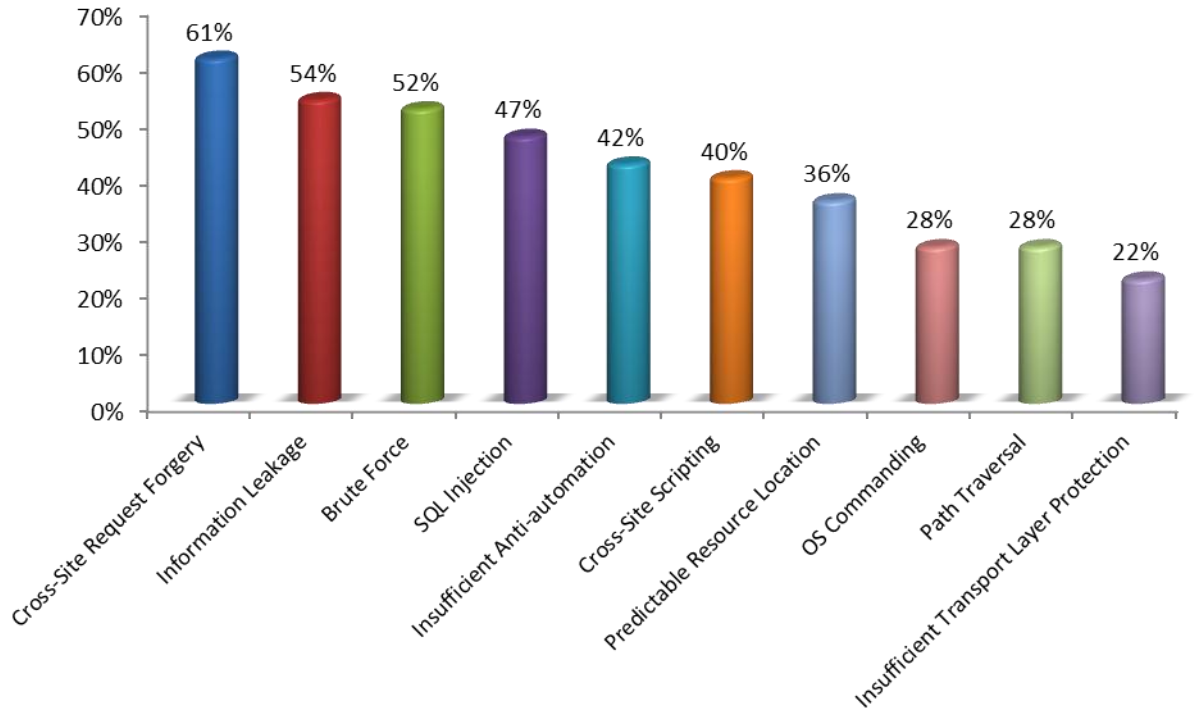

Рисунок 2. Наиболее распространенные уязвимости (доля сайтов, %)

На рис. 3 приведены данные по долям сайтов, на которых выявлены уязвимости различного уровня риска. Видно, что доля сайтов с уязвимостями высокой степени риска в 2011 году ниже по сравнению с 2010 годом, а средней степени — немного выше.

Наиболее распространенными уязвимостями высокой степени риска являются SQL Injection, OS Commanding и Path Traversal, которые встречаются практически в каждом третьем приложении.

Рисунок 3. Доли сайтов с уязвимостями (три уровня риска)

5.2. ПОКВАРТАЛЬНАЯ ДИНАМИКА

В данном разделе представлена динамика наличия уязвимостей разного типа и уровня риска на сайтах, детальный анализ защищенности которых был проведен в 2010—2011 годах.

Табл. 3 содержит поквартальные данные о количестве сайтов, в которых были обнаружены уязвимости высокого, среднего и низкого уровня риска. Эти данные графически представлены также на рис. 4. Доля сайтов, содержащих уязвимости с высоким уровнем риска, колеблется главным образом в интервале от 65% до 80%, спад этого показателя отмечен во II и IV кварталах 2011 года — до 50%, подъем — во II квартале 2010 года до значения в 85% сайтов и в IV квартале 2010 года до 91%. В целом в 2011 году протестированные приложения оказались более защищенными от атак с высокой степенью критичности. Почти во всех случаях на каждом сайте присутствует хотя бы одна уязвимость среднего уровня риска; ис-

ключение составили III и IV кварталы 2010 года: соответственно 91% и 82% сайтов с подобными уязвимостями. Доля сайтов, на которых обнаружены уязвимости низкого уровня риска, в 2011 году в среднем меньше, чем в 2010, однако в конце 2011 года вновь начинается подъем этого показателя.

Сокращение доли сайтов с критическими уязвимостями объясняется тем, что многие сайты в 2011 году проходили повторное тестирование после исправления недочетов, выявленных при предшествующем анализе защищенности.

Таблица 3. Динамика долей сайтов (%) с уязвимостями различной степени риска

Уровень риска	2010 I	2010 II	2010 III	2010 IV	2011 I	2011 II	2011 III	2011 IV
Высокий	67	85	64	91	64	50	65	50
Средний	100	100	91	82	100	100	100	100
Низкий	67	46	45	27	29	17	35	39

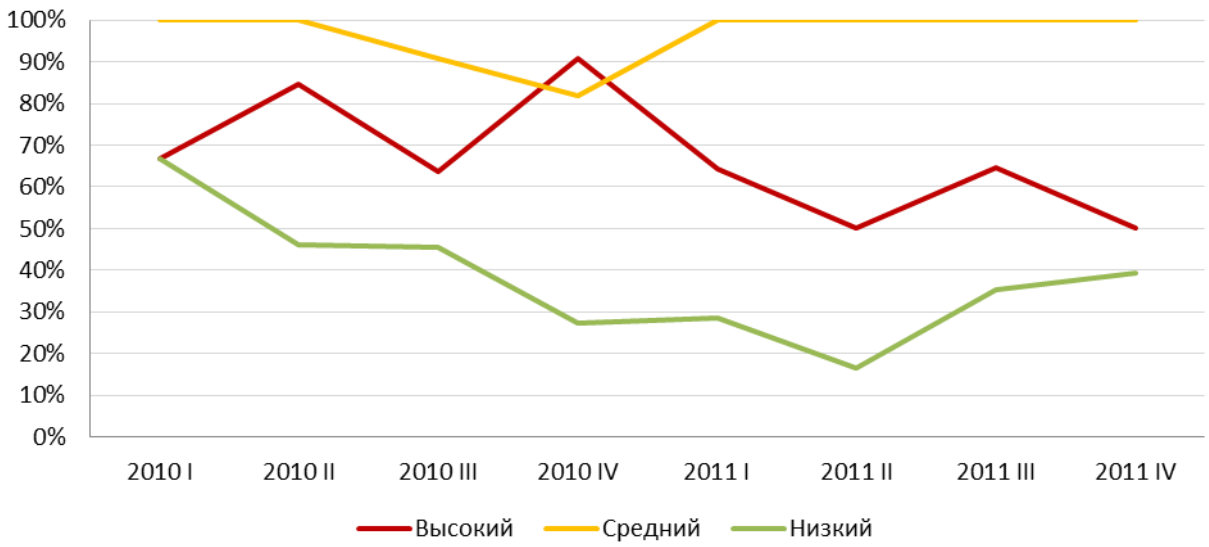

Рисунок 4. Динамика долей сайтов с уязвимостями различной степени риска

В табл. 4 и на рис. 5 приведены данные по долям сайтов, в которых обнаружены наиболее распространенные критические уязвимости. Лидером по количеству уязимых сайтов является SQL Injection. Пик распространения этой уязвимости наблюдается во II квартале 2010 года (77%). Динамика уровня защищенности от внедрения SQL-кода положительная: заметно, что в среднем в 2011 году данная уязвимость встречалась на тестируемых сайтах реже, чем в 2010 году.

Таблица 4. Динамика долей сайтов (%) с критическими уязвимостями

Уязвимость	**2010 I**	**2010 II**	**2010 III**	**2010 IV**	**2011 I**	**2011 II**	**2011 III**	**2011 IV**
SQL Injection	33	77	55	55	29	33	44	39
Path Traversal	67	8	18	36	21	50	44	11
OS Commanding	67	15	36	36	57	33	15	18
Remote File Inclusion	0	0	9	0	0	0	0	4

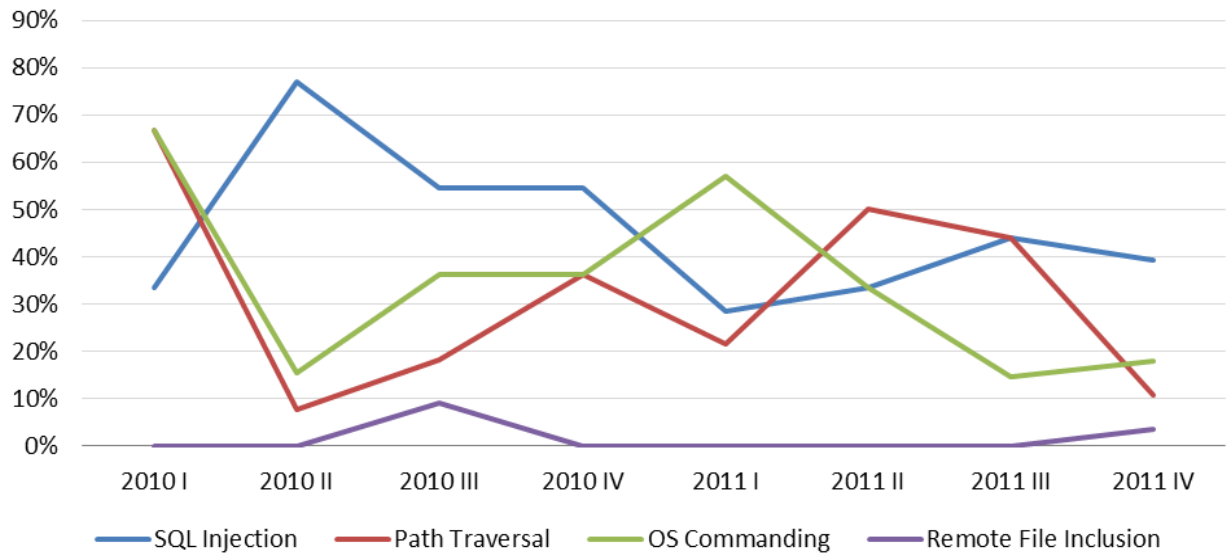

Рисунок 5. Динамика долей сайтов с критическими уязвимостями

В табл. 5 и на рис. 6 представлена динамика защищенности тестируемых приложений от межсайтового выполнения сценариев (Cross-Site Scripting, XSS). Доля ресурсов, подверженных соответствующей уязвимости, колеблется около значений 30—40% (лишь во II квартале 2010 года наблюдается пик в 69% сайтов).

Таблица 5. Динамика долей сайтов, уязвимых для XSS (в %)

Уязвимость	2010 I	2010 II	2010 III	2010 IV	2011 I	2011 II	2011 III	2011 IV
Cross-Site Scripting	33	69	36	27	36	50	32	43

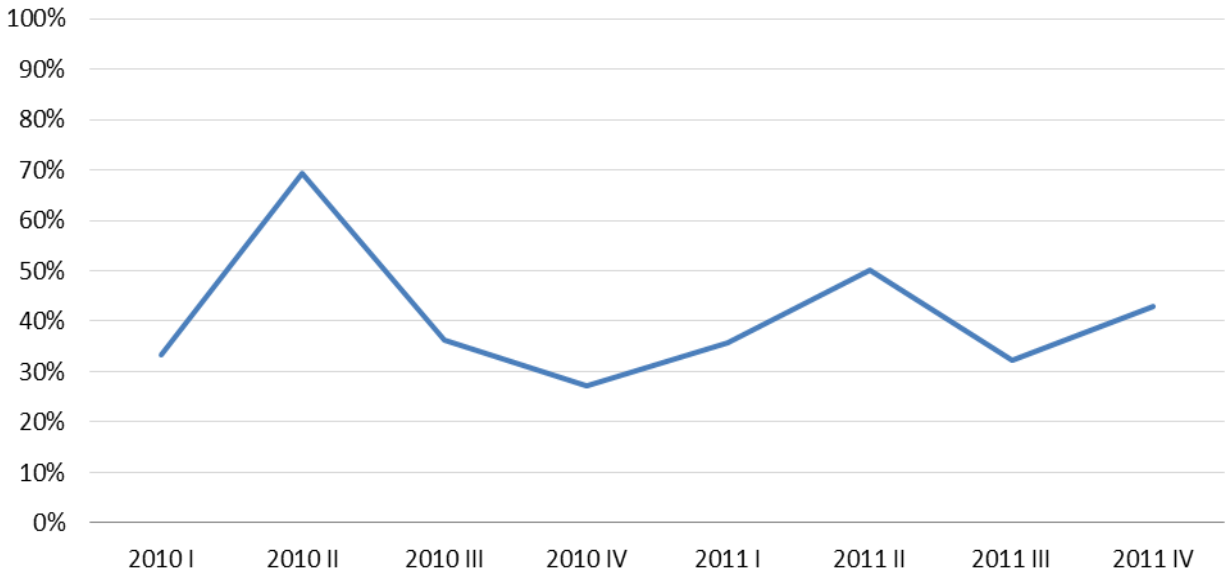

Рисунок 6. Динамика долей сайтов, уязвимых для XSS

Динамика подверженности Cross-Site Request Forgery приведена в табл. 6 и на рис. 7 и демонстрирует рост доли уязвимых сайтов (с 39% в среднем в 2010 году до 68% в 2011 году). Это связано со значительным повышением эффективности методов обнаружения данной уязвимости.

Таблица 6. Динамика долей сайтов, уязвимых для CSRF (в %)

Уязвимость	2010 I	2010 II	2010 III	2010 IV	2011 I	2011 II	2011 III	2011 IV
Cross-Site Request Forgery	33	69	36	18	79	50	71	71

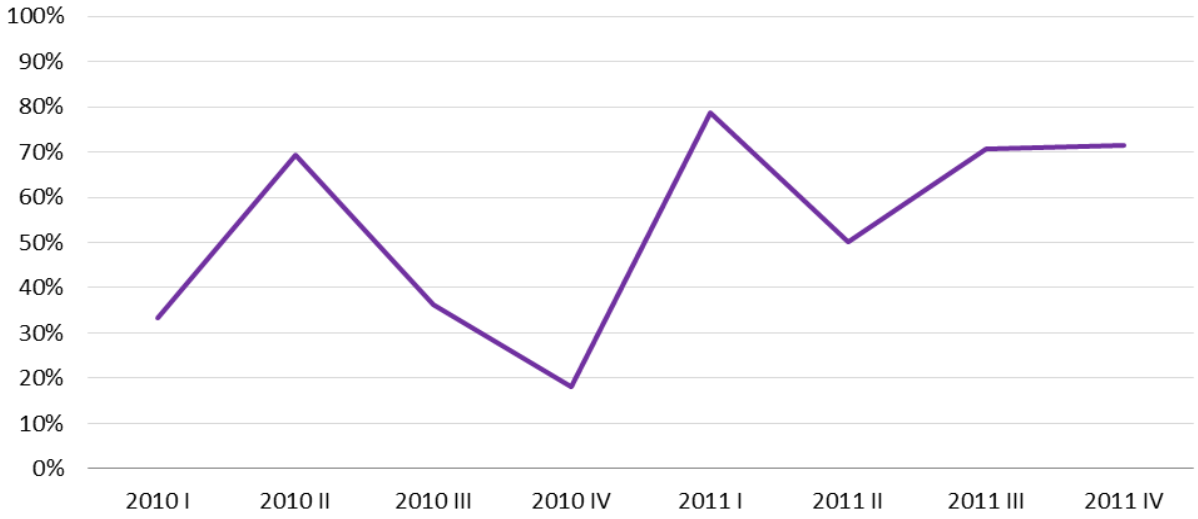

Рисунок 7. Динамика долей сайтов, уязвимых для CSRF

5.3. УЯЗВИМОСТИ, ХАРАКТЕРНЫЕ ДЛЯ РАЗЛИЧНЫХ ЯЗЫКОВ ПРОГРАММИРОВАНИЯ

Среди тестируемых ресурсов встречаются веб-приложения, написанные на различных языках программирования; при этом для каждого языка характерен свой набор наиболее значимых уязвимостей. Большинство разработчиков предпочли PHP: на нем написаны 63% всех протестированных сайтов. Значительны доли ASP.NET (19%) и Java (14%). Остальные языки программирования встречаются гораздо реже. Распределение сайтов — участников тестирования по лежащему в их основе языку программирования визуально представлено на рис. 8.

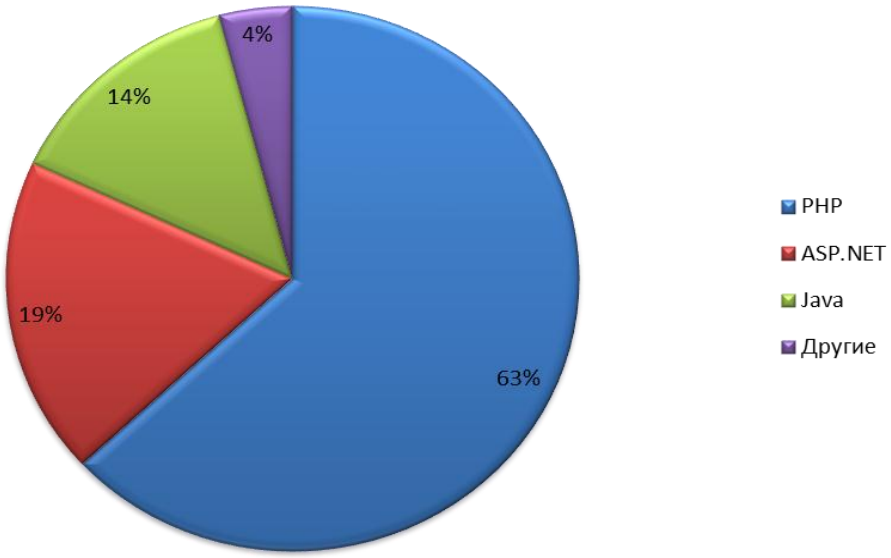

Рисунок 8. Распределение ресурсов по языку программирования

В табл. 7 приведено по пять уязвимостей с максимальной долей подверженных им сайтов — в зависимости от языка программирования. Среди веб-приложений, разработанных на языке PHP, наиболее часто встречаются следующие уязвимости: Cross Site Scripting, Cross-Site Request Forgery, Insufficient Anti-automation, а также две критические — SQL Injection и Path Traversal. Для платформы ASP.NET характерны те же самые уязвимости (исключение составляет Application Misconfiguration, занявшая место Path Traversal). В рейтинг среды Java вошли уязвимости Insufficient Authorization, Cross-Site Request Forgery, Application Misconfiguration, Insufficient Authentication и лишь одна критическая уязвимость — OS Commanding. Можно заметить, что доли уязвимых сайтов на ASP.NET и Java ниже по сравнению с аналогичными показателями для языка PHP.

Таблица 7. Наиболее распространенные уязвимости в зависимости от языка программирования

PHP	Доля сайтов, %	ASP.NET	Доля сайтов, %	Java	Доля сайтов, %
Cross-Site Request Forgery	73	Cross-Site Scripting	39	Insufficient Authorization	41
SQL Injection	61	Cross-Site Request Forgery	35	Cross-Site Request Forgery	35
Cross-Site Scripting	43	Insufficient Anti-automation	35	Application Misconfiguration	29
Insufficient Anti-automation	42	SQL Injection	22	Insufficient Authentication	29
Path Traversal	42	Application Misconfiguration	17	OS Commanding	29

На рис. 9 представлены данные по распределению критических и других распространенных уязвимостей, связанных с ошибками при разработке приложений. Числа указывают на доли сайтов, на которых выявлены соответствующие уязвимости. Среди сайтов на языке PHP доли ресурсов со всеми этими уязвимостями выше, что особенно характерно для SQL Injection (61% сайтов в сравнении с 22% на ASP.NET и 18% на Java) и Path Traversal (42% — при 18% у Java и отсутствии этой уязвимости на платформе ASP.NET). Уязвимость OS Commanding была обнаружена в 4% случаев на ASP.NET и в 29% случаев на Java. На этих платформах не выявлено ни одной уязвимости типа Null Byte Injection, в

отличие от PHP, для которого уязвимыми оказались 12% приложений. Доля PHP-сайтов, уязвимых для Cross-Site Request Forgery, составляет 73% и более чем в два раза превосходит данный показатель для ASP.NET и Java (по 35% сайтов).

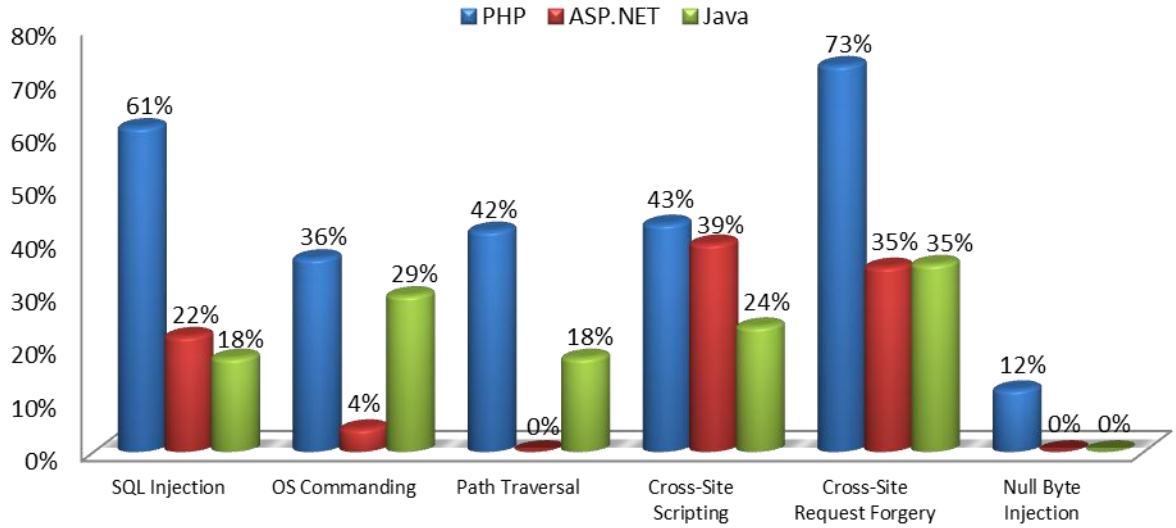

Рисунок 9. Доли сайтов на различных языках программирования с уязвимостями высокого и среднего уровня риска

В целом уязвимости с высокой степенью критичности чаще встречаются на PHP сайтах: 81% ресурсов (см. рис. 10) подвержены подобным проблемам.

Второе место занимает Java с 59%, и всего 26% сайтов на ASP.NET содержат уязвимости с высокой степенью риска. Различия по количеству ресурсов, содержащих уязвимости со средним и низким уровнем риска, незначительны.

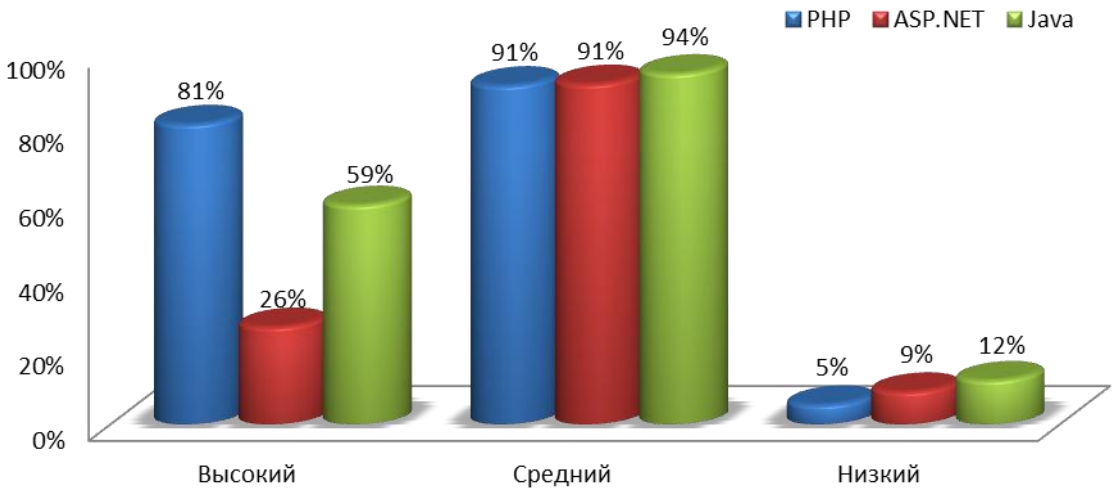

Рисунок 10. Доли сайтов на различных языках программирования с критическими уязвимостями

5.4. СРАВНЕНИЕ ХАРАКТЕРНЫХ УЯЗВИМОСТЕЙ В ЗАВИСИМОСТИ ОТ ВЕБ-СЕРВЕРА

Среди протестированных сайтов присутствуют приложения, функционирующие под управлением серверов Apache, Microsoft IIS, nginx, Jboss, Tomcat, IBM HTTP Server, Oracle Application Server и др. Однако только первые три представлены достаточно широко. Распределение сайтов по используемым веб-серверам приведено в табл. 8 и графически изображено на рис. 11. Видно, что участники тестирования предпочитают сервер Apache: его доля составляет более половины — 57%.

Таблица 8. Распределение сайтов по используемому веб-серверу

Сервер	Доля, %
Apache	57
IIS	17
Nginx	10
Другие	16

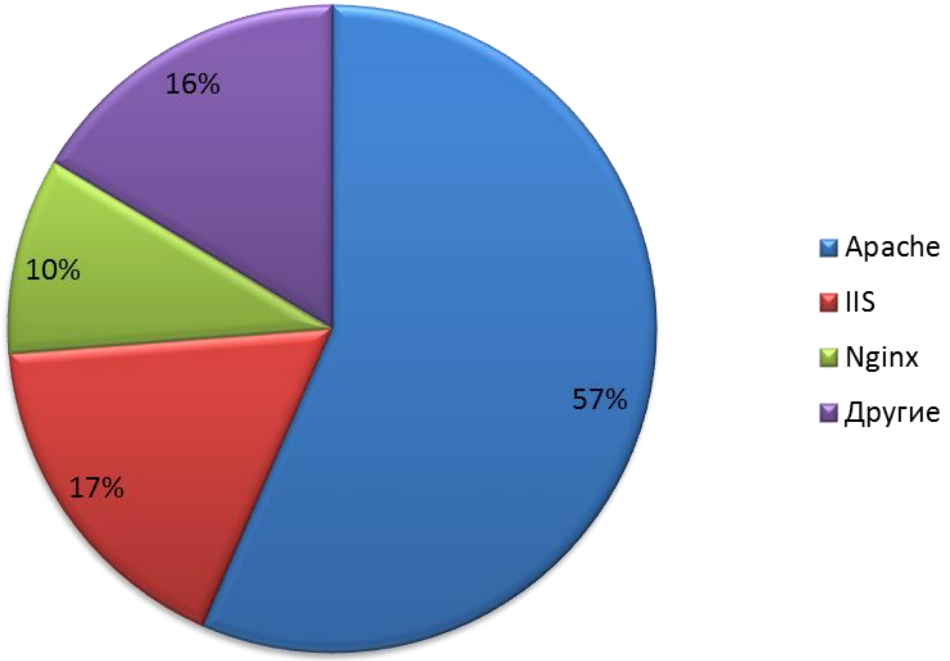

Рисунок 11. Распределение сайтов по используемому веб-серверу

Многие уязвимости веб-приложений, выделенные согласно классификации WASC TC v. 2, связаны с ошибками администрирования. В табл. 9 приведен рейтинг таких уязвимостей, отсортированных по доле уязвимых сайтов, которые работают под управлением Apache, Microsoft IIS, nginx и прочих веб-серверов. Во всех случаях лидером стала уязвимость Information Leakage. Кроме нее широко распространены также уязвимости Predictable Resource Location, Improper Filesystem Permissions и Insufficient Transport Layer Protection.

Таблица 9.1. Рейтинг уязвимостей, связанных с ошибками администрирования, для различных серверов

Apache	**Доля сайтов, %**	**IIS**	**Доля сайтов, %**
Information Leakage	54	Information Leakage	43
Predictable Resource Location	39	Insufficient Transport Layer Protection	29
Improper Filesystem Permissions	26	Improper Filesystem Permissions	5
Insufficient Transport Layer Protection	9	Predictable Resource Location	5
Directory Indexing	4	Server Misconfiguration	5
Insecure Indexing	3		
Server Misconfiguration	1		

Таблица 9.2. Рейтинг уязвимостей, связанных с ошибками администрирования, для различных серверов

Nginx	Доля сайтов, %	Другие	Доля сайтов, %
Information Leakage	83	Information Leakage	48
Insufficient Transport Layer Protection	75	Predictable Resource Location	38
Predictable Resource Location	67	Insufficient Transport Layer Protection	29
Improper Filesystem Permissions	33	Directory Indexing	10
Directory Indexing	25	Improper Filesystem Permissions	10
Server Misconfiguration	25	Server Misconfiguration	5
Insecure Indexing	8		

Более подробное сравнение по распространенным уязвимостям, связанным с конфигурацией и функционированием веб-серверов, приведено на рис. 12 и 13. Уязвимость Server Misconfiguration характерна для 25% сайтов, работающих под управлением nginx. Значительно меньше доли Apache и Microsoft IIS — 1% и 5% соответственно; кроме того, этой уязвимости подвержены в среднем 5% сайтов, построенных на прочих платформах. Уязвимость Improper Filesystem Permissions выявлена на 33% сайтах под управлением веб-сервера nginx, 26% под управлением Apache, 5% у Microsoft IIS и 10% для прочих веб-серверов. Insufficient Transport Layer Protection оказалась характерна для 75% систем с сервером nginx, 29% с Microsoft IIS, 9% с Apache, а также для 35% систем с другими серверами. Уязвимость Information Leakage была обнаружена на 83% ресурсов, использовавших веб-сервер nginx, на 54% для Apache, на 43% для Microsoft IIS и в 48% для всех прочих случаев.

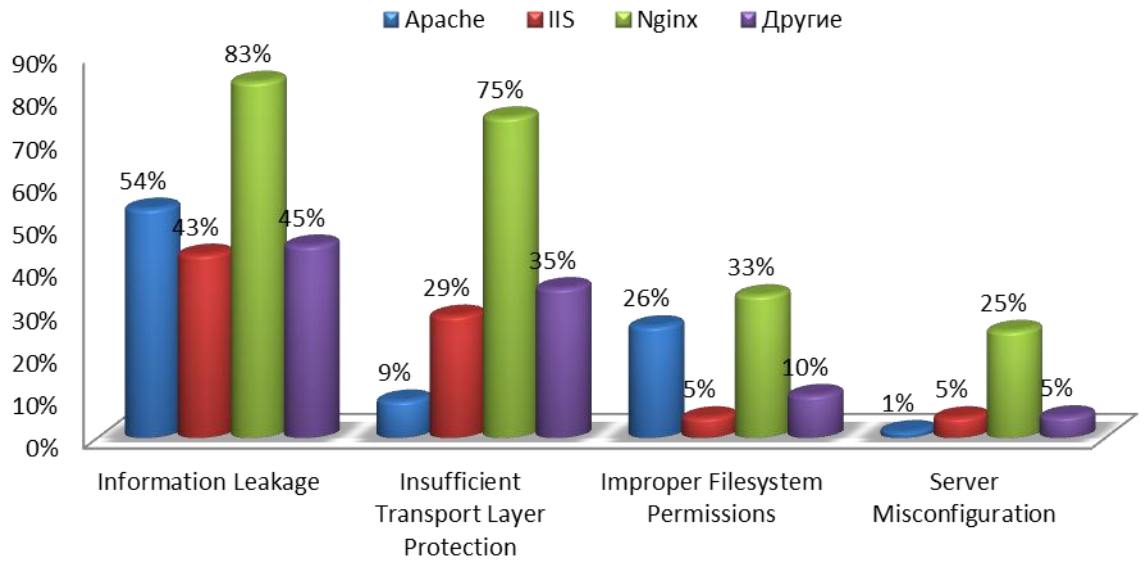

Рисунок 12. Доли уязвимых сайтов на различных веб-серверах

Уязвимость Predictable Resource Location присутствовала на 67% сайтах под управлением nginx, на 39% сайтов с Apache и лишь на 5% — с Microsoft IIS (см. рис. 13). Directory Indexing обнаружена на 25% ресурсах, использующих nginx, и на 4% сайтов, использующих Apache; данная уязвимость вовсе не была зафиксирована на сайтах, использующих Microsoft IIS. Не было выявлено среди сайтов под управлением веб-сервера IIS также и содержащих уязвимость Insecure Indexing, в то время как она была обнаружена на сайтах под управлением Apache (3%) и nginx (8%).

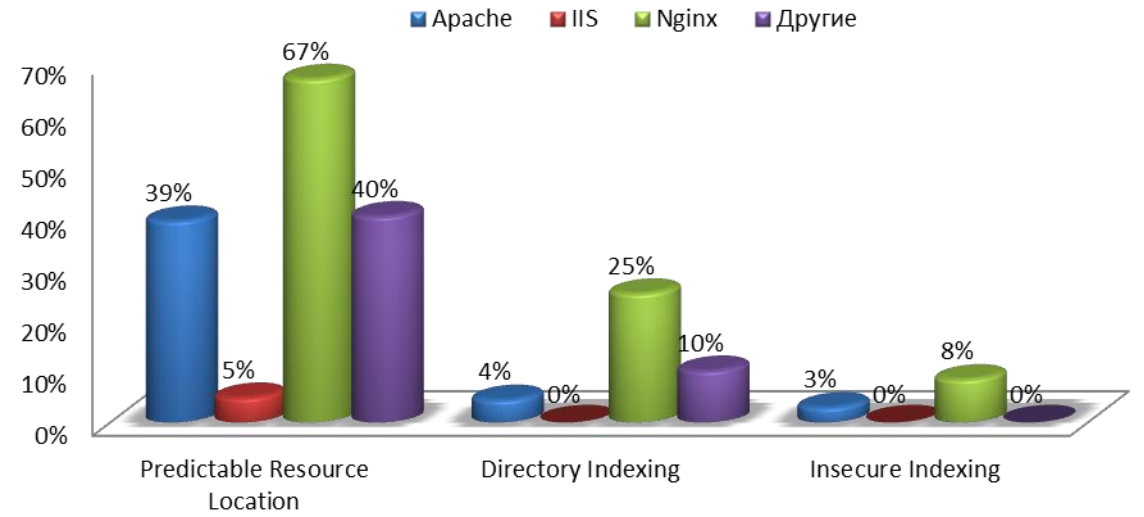

Рисунок 13. Доли уязвимых сайтов на различных веб-серверах (продолжение)

nginx превосходит все остальные веб-сервера по количеству уязвимых сайтов для всех типов уязвимостей, связанных с ошибками администрирования.

Минимальное количество уязвимостей связано с веб-сервером Microsoft IIS. Впрочем, приложения под управлением веб-сервера Microsoft IIS чаще других содержали недостатки Insufficient Transport Layer Protection и Server Misconfiguration по сравнению с приложениями под управлением веб-сервера Apache.

5.5. СРАВНЕНИЕ УЯЗВИМОСТЕЙ, ХАРАКТЕРНЫХ ДЛЯ РАЗЛИЧНЫХ ОТРАСЛЕЙ ЭКОНОМИКИ

Набор участников проведенного исследования позволяет оценить разницу в защищенности приложений в зависимости от отраслевой принадлежности владельца анализируемых систем. Разделение участников по отраслям экономики приведено на рис. 1 в разделе 4.

В зависимости от рода деятельности владельца и назначения системы наибольшую значимость могут приобретать конфиденциальность информации, или доступность ресурса, — или непременно и то, и другое. По областям экономики варьируется также и возможный ущерб от реализации атак. В итоге, для различных областей экономики значимы разные наборы уязвимостей, устранение которых становится первоочередной целью мероприятий по обеспечению информационной безопасности.

Опираясь на данные, представленные на рис. 14, можно сделать вывод:

Наибольшее внимание к защищенности своих ресурсов от критических уязвимостей проявляют владельцы сайтов из финансового и промышленного секторов

где доли приложений с такими уязвимостями составляют соответственно 43% и 50%. Почти 100% сайтов содержат уязвимости средней степени риска, но в промышленном секторе этот показатель снижается до 88%, а в сфере телекоммуникаций составляет 96%. Доля сайтов с уязвимостями низкой критичности значительно варьируется, лидером является финансовый сектор — 71%. Затем следует сфера информационных

технологий — 56% сайтов, промышленность — 38%, государственные организации — 23%, минимум наблюдается в сфере телекоммуникаций: всего 13% протестированных систем содержат уязвимости низкой степени риска.

Максимальное же число сайтов с уязвимостями высокого уровня риска наблюдалось в сфере телекоммуникаций — 88%.

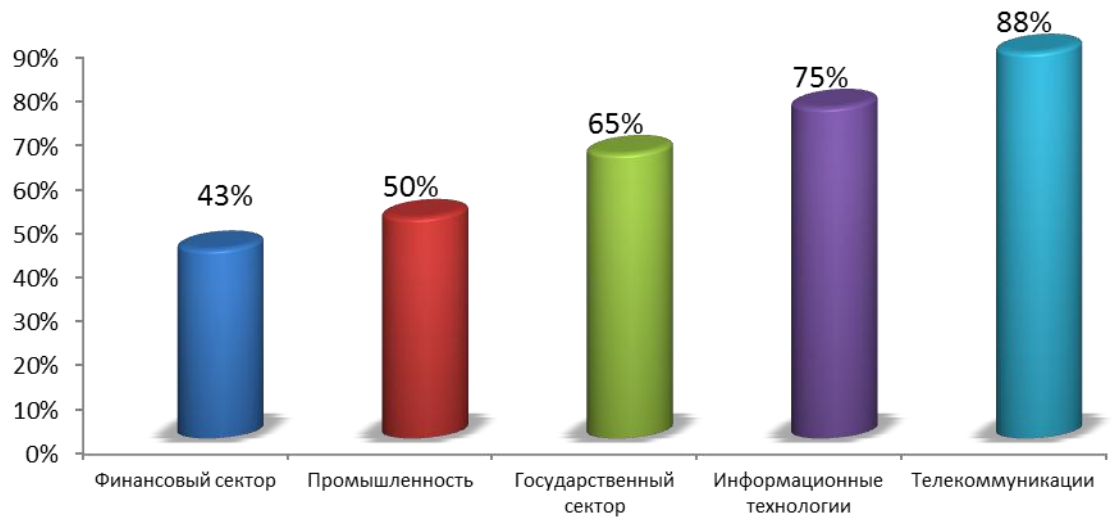

Рисунок 14. Доли сайтов с уязвимостями высокого уровня риска, принадлежащих разным отраслям экономики

Большое количество уязвимостей в телекоммуникационном секторе обусловлено пестрым разнообразием типов систем, которое зачастую становится следствием роста компаний, а также сделок по слиянию и поглощению.

Рис. 15 демонстрирует присутствие критических уязвимостей на сайтах из различных отраслей. Вновь заметен невысокий уровень уязвимости в сферах финансов и промышленности.

Рисунок 15. Доли уязвимых сайтов из различных отраслей экономики

Рис. 16 представляет разницу в распределении выявленных уязвимостей по уровню риска в отдельных экономических отраслях. Максимум критических уязвимостей наблюдается в сферах промышленности и информационных технологий. Ранее мы отмечали, что в промышленности критические уязвимости присутствуют на относительно небольшой части сайтов; их значительная доля при учете всех уязвимостей объясняется высокой концентрацией на тех сайтах, где они все-таки были обнаружены. В финансовом секторе критические уязвимости составляют наименьшую долю — всего 2%. Также относительно невелика их часть на сайтах государственного сектора (9%).

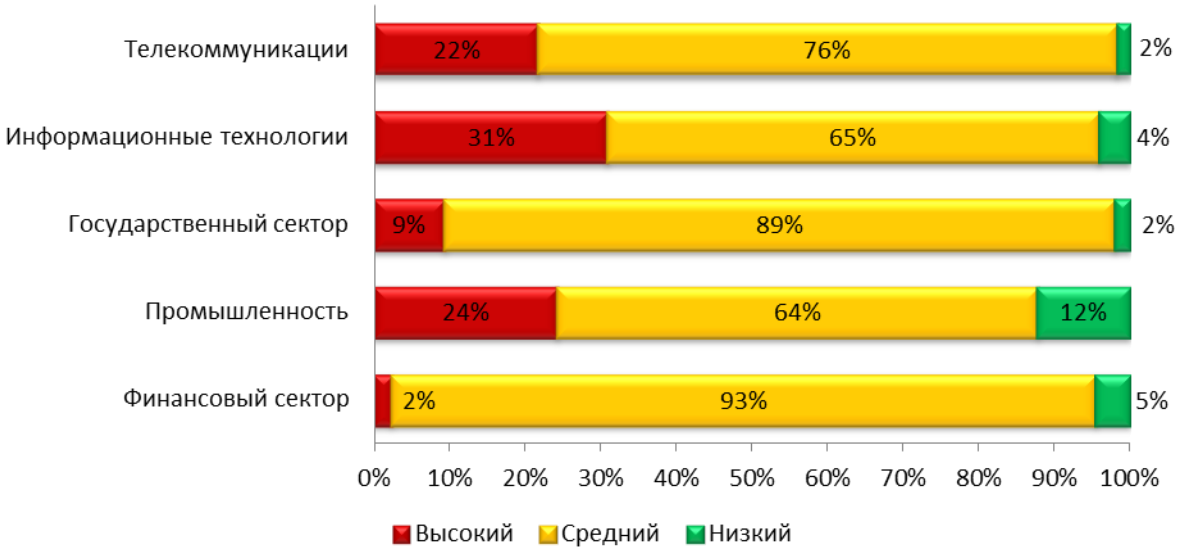

Рисунок 16. Распределение уязвимостей по уровню риска на сайтах из различных отраслей экономики

5.6. CMS И ХАРАКТЕРНЫЕ УЯЗВИМОСТИ

На большинстве протестированных веб-ресурсов используются коммерческие или свободные системы управления содержимым. Распределение сайтов по типам CMS приведено в табл. 10 и визуально продемонстрировано на рис. 17. Как видно, больше половины (58%) владельцев сайтов — участников исследования отдают предпочтение коммерческим системам; свободные CMS выбрали 25%, и 17% разрабатывали приложение самостоятельно.

Таблица 10. Распределение сайтов по типам CMS

Тип	Доля, %
Коммерческие	58
Свободные	25
Собственной разработки	17

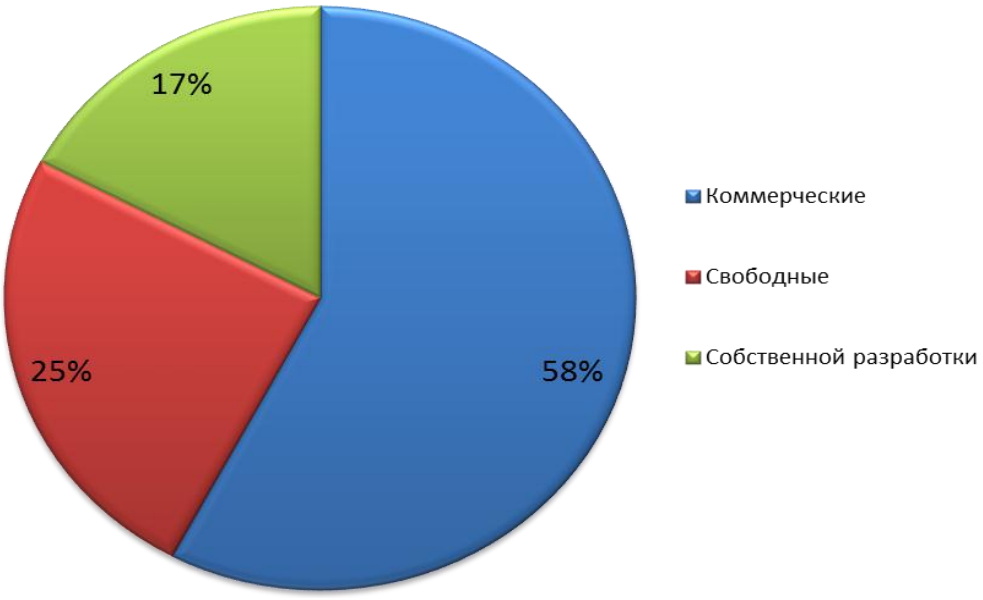

Рисунок 17. Распределение сайтов по типу CMS

Был проведен анализ характерных уязвимостей ресурсов с различными типами CMS (в табл. 11 приведены наиболее распространенные уязвимости). На сайтах, использующих коммерческие системы, чаще всего встречаются уязвимости Brute Force, Information Leakage, Cross-Site Request Forgery, Insufficient Anti-automation и SQL Injection. На сайтах со свободными CMS распространены Cross-Site Request Forgery, OS Commanding, Brute Force, Information Leakage и Cross-Site Scripting. В слу-

чае использования CMS собственной разработки — Cross-Site Request Forgery, Cross-Site Scripting, SQL Injection, Information Leakage и Predictable Resource Location.

Таблица 11. Наиболее распространенные уязвимости в зависимости от типа CMS

Коммерческие	Доля сайтов, %	Свободные	Доля сайтов, %	Собственной разработки	Доля сайтов, %
Brute Force	62	Cross-Site Request Forgery	55	Cross-Site Request Forgery	65
Information Leakage	62	OS Commanding	48	Cross-Site Scripting	65
Cross-Site Request Forgery	59	Brute Force	45	SQL Injection	60
Insufficient Anti-automation	55	Information Leakage	45	Information Leakage	50
SQL Injection	47	Cross-Site Scripting	38	Predictable Resource Location	50

На рис. 18 представлены данные о сайтах, содержащих уязвимости SQL Injection и OS Commanding, а также вредоносный код. Уязвимость SQL Injection выявлена на 60% ресурсов, использующих CMS собственной разработки, на 47% ресурсов с коммерческими CMS и 34% с бесплатными. OS Commanding — на 48% сайтов со свободными системами, 40% ресурсов с CMS собственного производства и 20% с коммерческими.

Вредоносным кодом оказались заражены 24% сайтов с бесплатными системами управления содержимым, 8% — с коммерческими и 5% — собственной разработки.

Различия в подверженности вредоносному коду объясняются относительной простотой создания вредоносного ПО для систем с открытым исходным кодом, а также широким использованием автоматических систем для проведения атак.

При этом системы собственной разработки, несмотря на наличие большого количества уязвимостей, менее подвержены «случайному» взлому при проведении массовой атаки с использованием автоматизированных средств.

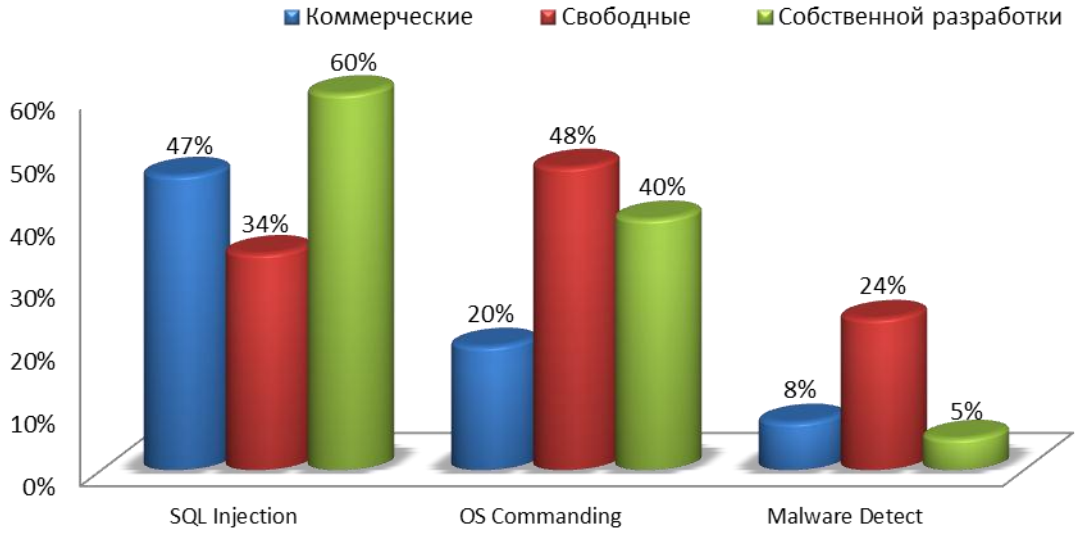

Рисунок 18. Сайты с различными типами CMS, содержащие критические уязвимости

Рис. 19 демонстрирует степень подверженности протестированных ресурсов атакам на клиент с учетом типа используемой системы управления содержимым. Уязвимости Cross-Site Scripting и Cross-Site Request Forgery преобладают на сайтах, где используется CMS собственной разработки. Значительные различия наблюдаются в распространенности уязвимости Cross-Site Scripting, которой подвержены 65% сайтов с CMS собственной разработки, 38% сайтов на базе бесплатных CMS и 33% — под управлением коммерческих. Различия в подверженности атаке Cross-Site Request Forgery невелики: незначительно большая доля уязвимых ресурсов принадлежит здесь CMS собственной разработки.

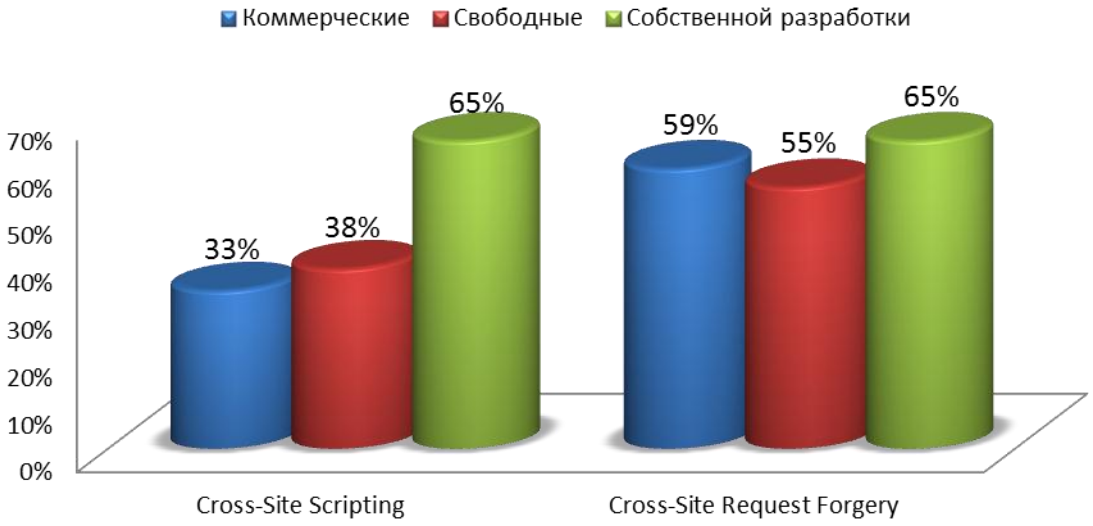

Рисунок 19. Сайты с различными типами CMS, содержащие распространенные уязвимости

На рис. 20 приводится сравнение ресурсов с различными типами CMS по степени распространенности уязвимостей Path Traversal, Remote File Inclusion и Null Byte Injection. Path Traversal заметно чаще встречался на сайтах с CMS собственной разработки (45%), чем на сайтах с коммерческими (29%) и бесплатными (28%) системами. Уязвимость Remote File Inclusion присутствовала только на ресурсах, использовавших CMS собственной разработки. Значительная доля сайтов с «собственными» CMS оказалась подвержена атаке Null Byte Injection (30%); со свободными и коммерческими системами — доли в 10% и 2% соответственно.

Практически по всем уязвимостям сайты с коммерческими системами управления содержимым показали высокий уровень защищенности.

Наименее защищенными оказались сайты с CMS собственной разработки (за исключением подверженности заражению вредоносным кодом).

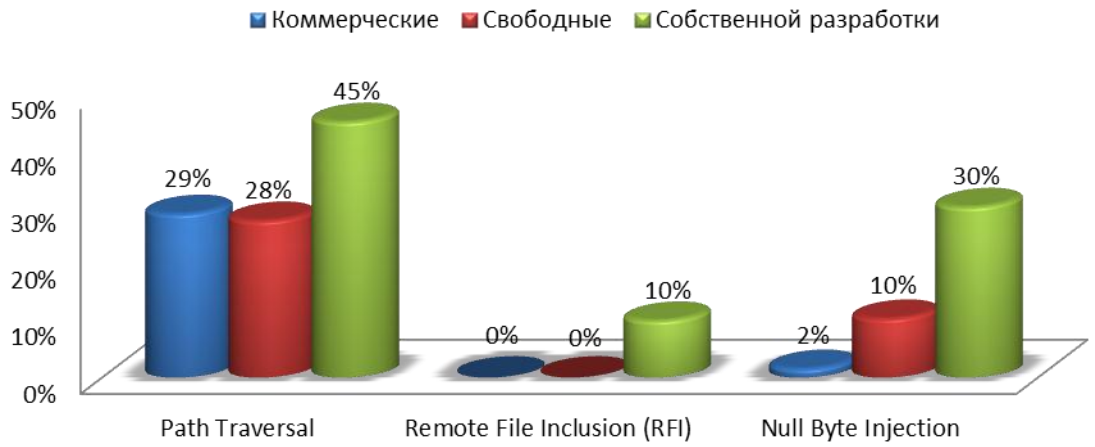

Рисунок 20. Сайты с различными типами CMS, содержащие критические уязвимости

При анализе распределения обнаруженных уязвимостей по уровням риска (рис. 21) мы обнаружили, что доли критических уязвимостей на сайтах, использующих свободные системы управления содержимым или системы собственной разработки, составляют по 25% и значительно превышают долю критических уязвимостей на сайтах с коммерческими CMS, которая составляет 7%.

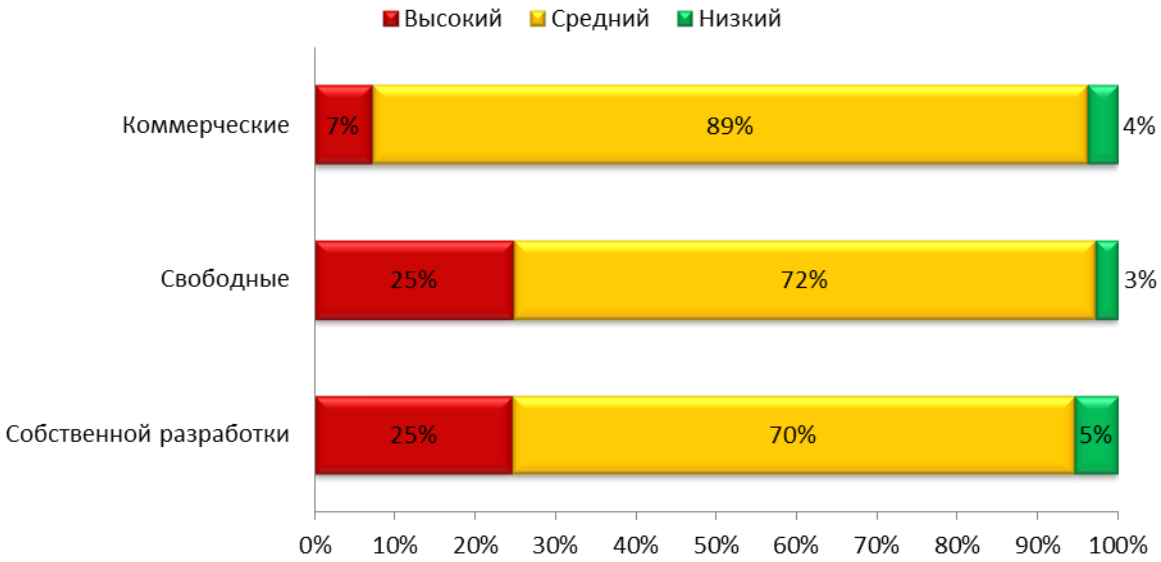

Рисунок 21. Распределение уязвимостей по уровням риска на сайтах с различными типами CMS

5.7. АНАЛИЗ ЗАЩИЩЕННОСТИ САЙТОВ С ВРЕДОНОСНЫМ КОДОМ

В ходе исследования отдельно были рассмотрены ресурсы, на которых обнаружилось наличие вредоносного кода. Их доля, как можно видеть на рис. 22, составила 10%.

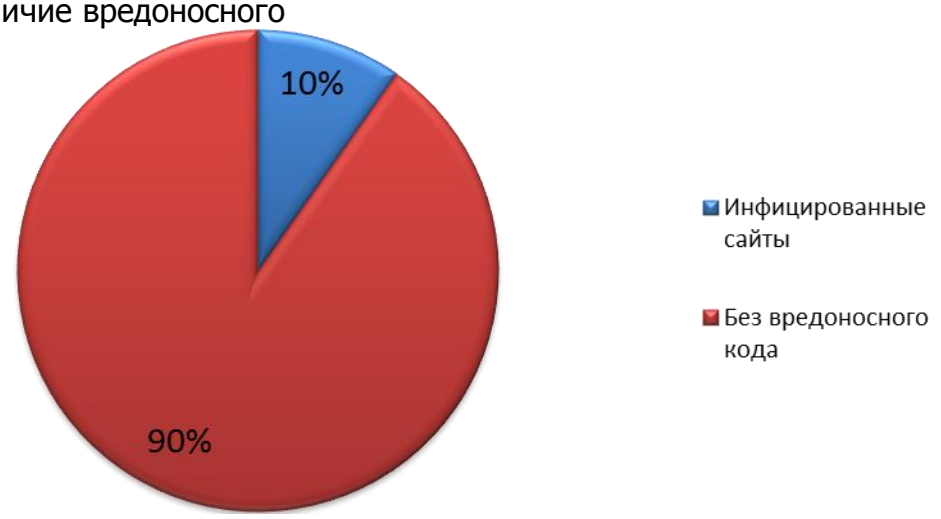

Рисунок 22. Доля сайтов с вредоносным кодом

В табл. 12 приведено распределение ресурсов, на которых выявлен вредоносный код, по языку программирования и типам используемых CMS. Половина зараженных сайтов работает под управлением свободных CMS.

Практически все сайты, зараженные вредоносным кодом (92%), — написаны на языке PHP и работают под управлением веб-сервера Apache.

Таблица 12. Распределение ресурсов с вредоносным кодом в зависимости от языка программирования и типа CMS

	Коммерческая CMS	Свободная CMS	CMS собственной разработки
PHP	34%	50%	8%
ASP.NET	—	—	—
Java	8%	—	—

В табл. 13 приведены наиболее распространенные уязвимости сайтов с вредоносным кодом. В список вошли уязвимости OS Commanding (92% уязвимых сайтов), Cross-Site Request Forgery (75%), SQL Injection (58%), Improper Filesystem Permissions (50%) и Cross-Site Scripting (42%).

Перечень уязвимостей для сайтов без вредоносного кода значительно отличается: Cross-Site Request Forgery (59%), Brute Force (56%), Information Leakage (53%), SQL Injection (44%) и Insufficient Anti-automation (43%).

Таблица 13. Уязвимости, наиболее распространенные на сайтах с вредоносным кодом

С вредоносным кодом	Доля сайтов, %	Без вредоносного кода	Доля сайтов, %
OS Commanding	92	Cross-Site Request Forgery	59
Cross-Site Request Forgery	75	Brute Force	56
SQL Injection	58	Information Leakage	53
Improper Filesystem Permissions	50	SQL Injection	44
Cross-Site Scripting	42	Insufficient Anti-automation	43

На рис. 23 приведено сравнение по распределению уязвимостей на сайтах с вредоносным кодом и без него.

Треть всех ресурсов, содержащих эту уязвимость, была заражена. Заметны различия в долях сайтов, со-

держащих уязвимость Improper Filesystem Permissions: 50% зараженных и 17% не инфицированных узлов. Уязвимы для SQL Injection оказались сайты с вредоносным кодом в 58% случаев, сайты без такового — в 44% случаев. Итак, можно утверждать, что наличие уязвимостей OS Commanding и Improper Filesystem Permissions способствует заражению информационного ресурса.

92% сайтов с вредоносным кодом оказались уязвимы к атаке OS Commanding.

Рисунок 23. Распределение уязвимостей в зависимости от наличия вредоносного кода

5.8. АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМ ДБО

Отдельным объектом исследования стали сайты дистанционного банковского обслуживания — системы, наиболее чувствительные к проблемам информационной безопасности. В табл. 14 приведен список выявленных уязвимостей с указанием соответствующей доли уязвимостей ДБО — участников исследования. Самой распространенной уязвимостью оказалась Insufficient Authorization.

Таблица 14. Распределение уязвимостей на сайтах систем ДБО

Уязвимость	Доля уязвимостей, %
Insufficient Authorization	31

Cross-Site Scripting	18
Fingerprinting	9
Predictable Resource Location	8
Cross-Site Request Forgery	6
Information Leakage	6
Insufficient Authentication	5
Insufficient Anti-automation	4
Brute Force	3
Credential/Session Prediction	3
Abuse of Functionality	2
Content Spoofing	2
Insufficient Transport Layer Protection	2
Directory Indexing	1
Insufficient Session Expiration	1
Path Traversal	1

Обнаруженные на сайтах ДБО критические уязвимости составляют лишь 1% от общего числа, что значительно меньше среднего показателя (13%).

Как видно на рис. 24, уязвимостей с низкой степенью критичности также немного — 9%. Основная часть выявленных уязвимостей (90%) связана со средним уровнем риска.

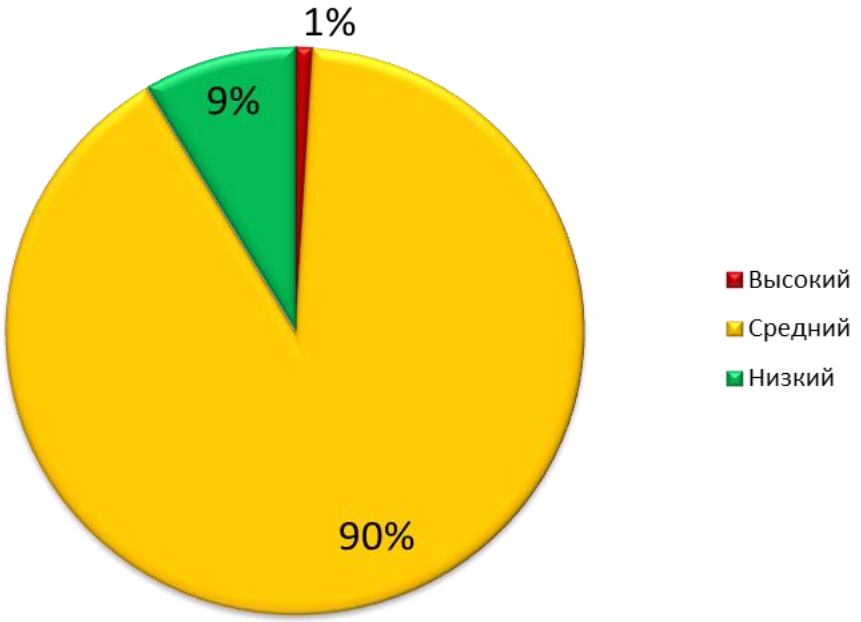

Рисунок 24. Распределение уязвимостей различного уровня риска на сайтах ДБО

5.9. АНАЛИЗ ДАННЫХ В КОНТЕКСТЕ ТРЕБОВАНИЙ PCI DSS

В настоящем разделе приводится анализ соответствия протестированных систем финансового сектора требованиям стандарта PCI DSS v. 2 [3]. Здесь представлены данные не только по системам ДБО, но и по другим веб-приложениям, попадающим в область действия стандарта. В табл. 15 перечислены требования стандарта, регламентирующие обязательное устранение конкретных уязвимостей в веб-приложениях.

Таблица 15. Требования стандарта PCI DSS v. 2

Требование	Процедура
6.5.1 Внедрение кода, в частности SQL-кода. К подобным атакам также относится внедрение команд ОС, операторов LDAP и Xpath и др.	Необходимо проверять входную информацию и следить за тем, чтобы данные, вводимые пользователем, не могли влиять на значения команд, использоваться в параметризованных запросах и др.
6.5.2 Переполнение буфера	Необходимо проверять границы буфера и усекать вводимые строки

6.5.3 Небезопасное хранение материалов шифрования	Необходимо обеспечить отсутствие уязвимостей шифрования
6.5.4 Небезопасная передача информации	Необходимо реализовать надежное шифрование данных аутентификации и других важных данных при их передаче
6.5.5 Некорректная обработка ошибок	Необходимо не допускать утечки данных в сообщениях об ошибках
6.5.7 Межсайтовое выполнение сценариев	Необходимо проверять все параметры перед их включением в код, использовать контекстно-зависимое экранирование символов.
6.5.8 Некорректное управление доступом, например небезопасные прямые объектные ссылки, отсутствие ограничения доступа по URL-адресу и обход каталога	Необходимо реализовать корректную аутентификацию пользователей и очищение вводимой информации; пользователи не должны иметь доступ к ссылкам на внутренние объекты
6.5.9 Межсайтовая подмена запросов	Необходимо не допускать автоматической отправки браузером данных аутентификации и идентификаторов сессии

Только 10% приложений полностью удовлетворяют требованиям PCI DSS к защите веб-ресурсов.

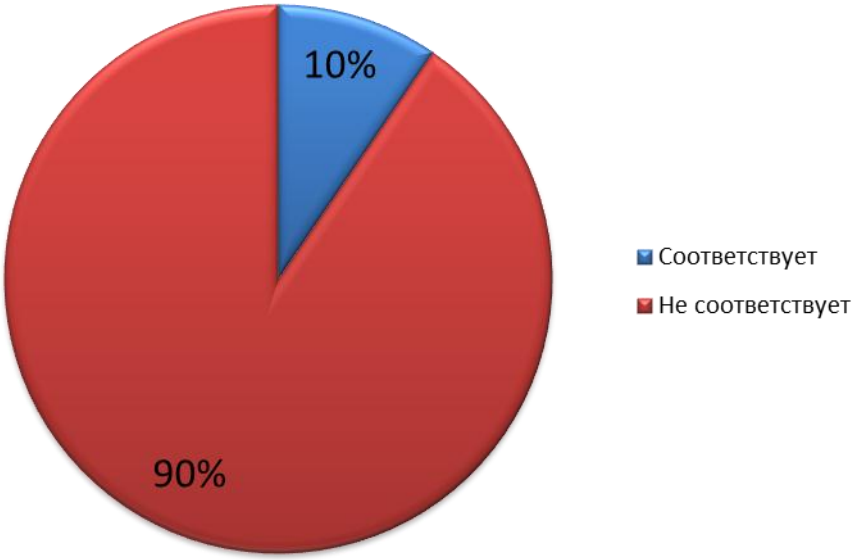

Рисунок 25. Доля сайтов, соответствующих требованиям PCI DSS

На рис. 26 представлены доли сайтов с уязвимостями, противоречащими требованиям стандарта PCI DSS по защите веб-приложений, которые перечислены в табл. 12, — отдельно для каждого требования. Около 24% сайтов оказались подвержены атакам внедрения различных элементов, среди которых, по общим данным, наиболее распространено внедрение SQL-кода. Лидером по количеству несоответствующих ресурсов стало требование 6.5.5: на 76% сайтов происходит утечка информации в результате некорректной обработки ошибок.

Распространенные уязвимости к атакам Cross-Site Scripting и Cross-Site Request Forgery присутствовали соответственно на 52% и 43% тестируемых сайтов.

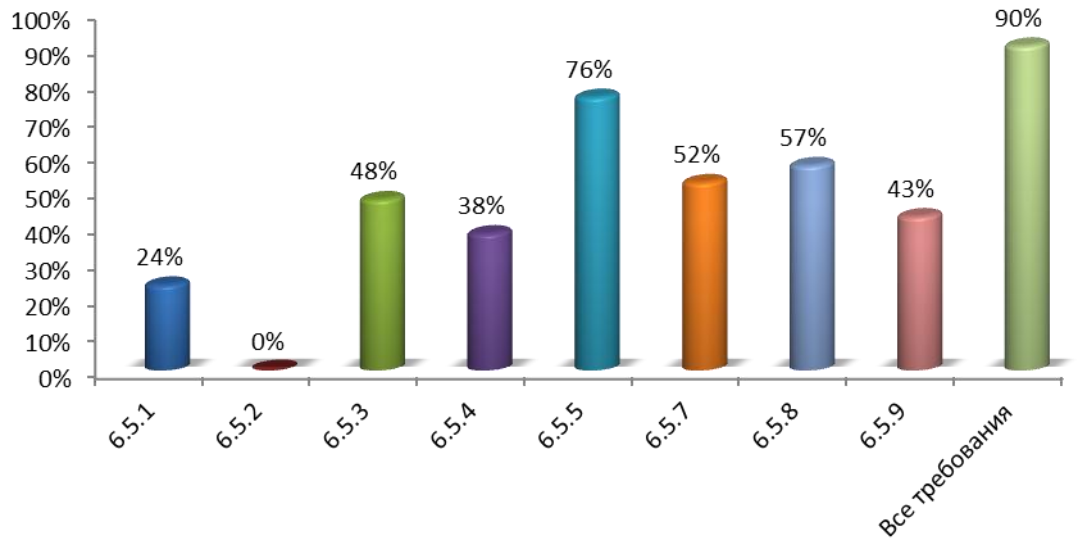

Рисунок 26. Доли сайтов, не соответствующих отдельным требованиям PCI DSS

Общая доля сайтов финансового сектора, не соответствующих требованиям 6.5.1—6.5.5, 6.5.7—6.5.9, составила 90%.

6. О КОМПАНИИ

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Компания входит в число наиболее динамично развивающихся участников рынка ИТ, демонстрируя ежегодный рост более 50%. Офисы и представительства Positive Technologies расположены в Москве, Лондоне, Риме, Сеуле и Тунисе.

Разработанные экспертами компании программные продукты заслужили международное признание в сфере практической информационной безопасности.

Продукты

Система контроля защищенности и соответствия стандартам MaxPatrol помогает обеспечивать безопасность корпоративных информационных систем и формировать комплексное представление о реальном уровне защищенности IT-инфраструктуры организации. Система позволяет контролировать выполнение требований государственных, отраслевых и международных стандартов, таких как Федеральный закон № 152-ФЗ «О персональных данных», СТО БР ИББС, ISO 27001/27002, SOX 404, PCI DSS. В MaxPatrol объединены активные механизмы оценки защищенности, включая функции системных проверок, тестирования на проникновение, контроля соответствия стандартам — в сочетании с поддержкой анализа различных операционных систем, СУБД и веб-приложений.

Система анализа защищенности XSpider более 10 лет является признанным лидером среди средств сетевого аудита ИБ. На сегодняшний день это один из лучших интеллектуальных сканеров безопасности в мире. Более 1000 международных компаний успешно используют XSpider для анализа и контроля защищенности корпоративных ресурсов.

Услуги

Компания Positive Technologies специализируется на проведении комплексного аудита информационной безопасности, на оценке защищенности прикладных систем и веб-приложений, тестировании на проникновение и внедрении процессов мониторинга информационной безопасности. Статус PCI DSS Approved Scanning Vendor позволяет проводить работы по проверке соответствия данному стандарту.

Исследования

Positive Research — один из крупнейших в Европе исследовательских центров в области информационной безопасности. В его задачи входит анализ передовых тенденций IT-индустрии, а также их использование для развития продуктов и сервисов компании. Эксперты центра проводят исследовательские и конструкторские работы, анализ угроз и уязвимостей, содействуют разработчикам в устранении ошибок в различных системах и приложениях.

Лицензии

Свою деятельность Positive Technologies осуществляет на основе лицензий ФСБ, ФСТЭК и Министерства обороны РФ. Продукты компании сертифицированы ФСТЭК, Минобороны и ОАО «Газпром» (по системе ГАЗПРОМСЕРТ), а ее специалисты участвуют в работе различных международных ассоциаций: Web Application Security Consortium, (ISC)², ISACA, Certified Ethical Hacker, Center for Internet Security.

Клиенты

В числе заказчиков Positive Technologies — более 1000 государственных учреждений, финансовых организаций, телекоммуникационных и розничных компаний, промышленных предприятий России, стран СНГ и Балтии, а также Великобритании, Германии, Голландии, Израиля, Ирана, Китая, Мексики, США, Таиланда, Турции, Эквадора, ЮАР и Японии.

Вклад в развитие индустрии

Принимая активное участие в жизни отрасли, Positive Technologies выступает организатором международного форума по информационной безопасности Positive Hack Days и развивает SecurityLab — самый популярный русскоязычный портал о ИБ.

7. ССЫЛКИ

1. WASC Threat Classification v. 2.0: http://projects.webappsec.org/Threat-Classification.
2. Common Vulnerability Scoring System: http://www.first.org/cvss.
3. PCI Data Security Standard: https://www.pcisecuritystandards.org/security_standards/index.php.
4. OWASP Top Ten Project: https://www.owasp.org/index.php/OWASP_Top_Ten_Project.

8. ПРИЛОЖЕНИЯ

Приложение А. Методика оценки степени риска

Таблица А.1. Методика оценки степени риска

Классификация угроз	Базовая оценка по шкале CVSS
Abuse of Functionality	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Brute Force Attack	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Buffer Overflow	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Content Spoofing	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Credential/Session Prediction	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Cross-Site Scripting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
Cross-Site Request Forgery	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Denial of Service	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
Format String Attack	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
HTTP Request Splitting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
HTTP Response Splitting	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
HTTP Request Smuggling	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
HTTP Response Smuggling	6.4 (AV:N/AC:L/Au:N/C:P/I:P/A:N)
Integer Overflow	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
LDAP Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Mail Command Injection	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
Null Byte Injection	5 (AV:N/AC:L/Au:N/C:N/I:P/A:N)
OS Commanding	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Path Traversal	7.8 (AV:N/AC:L/Au:N/C:C/I:N/A:N)
Predictable Resource Location	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Remote File Inclusion	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Routing Detour	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
SOAP Array Abuse	7.8 (AV:N/AC:L/Au:N/C:N/I:N/A:C)
SSI Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Session Fixation	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
SQL Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
URL Redirectors	2.6 (AV:N/AC:H/Au:N/C:N/I:P/A:N)
XPath Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)

XML Attribute Blowup	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
XML External Entity	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
XML Entity Expansion	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
XML Injection	7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)
XQuery Injection	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Application Misconfiguration	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
Directory Indexing	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Fingerprinting	0 (AV:N/AC:L/Au:N/C:N/I:N/A:N)
Improper Parsing	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Improper Permissions	10 (AV:N/AC:L/Au:N/C:C/I:C/A:C)
Information leakage	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Insecure Indexing	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Insufficient Anti-automation	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Insufficient Authentication	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Insufficient Authorization	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Insufficient Data Protection	5 (AV:N/AC:L/Au:N/C:P/I:N/A:N)
Insufficient Password Recovery	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
Insufficient Process Validation	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Insufficient Session Expiration	6.8 (AV:N/AC:M/Au:N/C:P/I:P/A:P)
Insufficient Transport Layer Protection	4 (AV:N/AC:H/Au:N/C:P/I:P/A:N)
Server Misconfiguration	5.1 (AV:N/AC:H/Au:N/C:P/I:P/A:P)
Improper File System Permissions	4.4 (AV:L/AC:M/Au:N/C:P/I:P/A:P)

Приложение B. Распространенность уязвимостей

Таблица B.1. Распределение уязвимостей долям сайтов

Тип уязвимости	Доля уязвимости, %	Доля сайтов, %
Abuse of Functionality	0,33	4,88
Application Misconfiguration	2	17,07
Brute Force	35,48	52,03
Buffer Overflow	0	0
Content Spoofing	0,39	4,88
Credential/Session Prediction	1,22	8,13
Cross-Site Request Forgery	4,77	60,98
Cross-Site Scripting	14,30	39,84
Directory Indexing	0,44	6,50
Fingerprinting	3,27	34,15
Format String	0	0
HTTP Request Smuggling	0	0
HTTP Request Splitting	0,28	0,81
HTTP Response Smuggling	0,06	0,81
HTTP Response Splitting	0,11	1,63
Improper Filesystem Permissions	1,61	20,33
Information Leakage	7,15	53,66
Insecure Indexing	0,17	2,44
Insufficient Anti-automation	3,27	42,28
Insufficient Authentication	1,77	16,26
Insufficient Authorization	2,61	11,38
Insufficient Process Validation	0	0
Insufficient Session Expiration	0,28	4,07
Insufficient Transport Layer Protection	1,55	21,95
Integer Overflows	0	0
LDAP Injection	0	0
Mail Command Injection	0,06	0,81
Null Byte Injection	0,55	7,32

OS Commanding	2,44	27,64
Path Traversal	2,44	27,64
Predictable Resource Location	4,66	35,77
Remote File Inclusion	0,17	1,63
Routing Detour	0	0
Server Misconfiguration	0,33	4,88
Session Fixation	0,67	9,76
SOAP Array Abuse	0	0
SQL Injection	6,82	45,53
SSI Injection	0	0
URL Redirector Abuse	0,5	6,5
XML Attribute Blowup	0	0
XML Entity Expansion	0	0
XML External Entities	0,11	0,81
XML Injection	0	0
XPath Injection	0,06	0,81
XQuery Injection	0	0
Insufficient Password Recovery	0,17	2,44
Malware Detect	0,83	9,76

www.ptsecurity.ru
pt@ptsecurity.ru
+7 (495) 744 01 44