DOI 10.37882/2223-2966.2024.7-2.20

АНАЛИЗ И ПРОГНОЗИРОВАНИЕ УГРОЗ КИБЕРБЕЗОПАСНОСТИ

ANALYSIS AND FORECASTING OF CYBERSECURITY THREATS

D. Makarov
A. Tsaregorodtsev
I. Mukhin
S. Volkov

Summary. In the era of widespread digitalization and the development of information technologies, leading to the emergence of new threats to information security (IS), and cybersecurity, software vulnerabilities are becoming an even more significant threat to both organizations and individual users. The article conducts research and analysis of software errors and vulnerabilities in the period from 2020 to 2023, based on data from CWE (Common Weakness Enumeration) and OpenCVE (Open-Source Computer Vision Library) in the period from 2020 to 2023, and provides a forecast of trends in the development of software vulnerabilities. The identification of key trends in software vulnerabilities is considered, their potential impact in the future is assessed, and strategies for effective response to these threats are proposed. The methodology includes the analysis of lists of the 25 most dangerous software security vulnerabilities and the use of predictive analytics to assess risks. Visualized data and analytical conclusions are presented to identify key risk areas, based on which recommendations are proposed to improve the cybersecurity of the enterprise.

Keywords: cybersecurity, software vulnerabilities, predictive analytics, information security risk assessment, threat forecasting.

Макаров Дмитрий Александрович
Аспирант, ФГБОУ ВО Московский государственный лингвистический университет
MakarovPostOffice@yandex.ru
Царегородцев Анатолий Валерьевич
доктор технических наук, профессор, директор, ФГАОУ ВО Российский университет дружбы народов г. Москва
tsaregorodtsev_av@pfur.ru
Мухин Илья Николаевич
Специалист, старший преподаватель, ФГАОУ ВО Российский университет дружбы народов г. Москва
mukhin_in@pfur.ru
Волков Сергей Дмитриевич
Заместитель директора, ФГАОУ ВО Российский университет дружбы народов г. Москва
volkov_sd@pfur.ru

Аннотация. В эпоху повсеместной цифровизации и развития информационных технологий, приводящих к появлению новых угроз информационной безопасности (ИБ), и, в частности, кибербезопасности, уязвимости программного обеспечения (ПО) становятся еще более значительной угрозой как для организаций, так и для индивидуальных пользователей. В статье проводится исследование и анализ ошибок и уязвимостей ПО в период с 2020 по 2023 год, на основе данных CWE (Common Weakness Enumeration) и OpenCVE (Open Source Computer Vision Library) в период с 2020 по 2023 годы, и даётся прогноз тенденций развития уязвимостей ПО. Рассматривается идентификация ключевых тенденций уязвимостей ПО, даётся оценка их потенциального влияния в будущем, и предлагаются стратегии для эффективного реагирования на эти угрозы. Методология включает анализ списков 25 самых опасных программных уязвимостей безопасности и применение предиктивной аналитики для оценки рисков. Представлены визуализированные данные и аналитические заключения, позволяющие выявить ключевые области рисков, на основе которых предлагаются рекомендации для повышения кибербезопасности предприятия.

Ключевые слова: кибербезопасность, уязвимости ПО, предиктивная аналитика, оценка рисков ИБ, прогнозирование угроз.

Введение

В современном мире, где цифровые технологии проникают во все аспекты нашей жизни, безопасность программного обеспечения становится одним из приоритетов. Уязвимости в ПО не только создают риски для безопасности данных и конфиденциальности, но и могут привести к серьезным экономическим и социальным последствиям. С развитием технологий и постоянно меняющимся ландшафтом угроз, важно не только реагировать на текущие вызовы, но и прогнозировать уязвимости ПО. Прогнозирование потенциальных угроз в области кибербезопасности проводилось на основе анализа ошибок и тенденций уязвимостей ПО с 2020 по 2023 годы. Упор делался на данные, предоставленные CWE, а в качестве дополнительных ресурсов использовалась платформа OpenCVE для более углубленного изучения и прогнозирования уязвимостей ПО. Для оценки рисков, которые эти уязвимости могут представлять в будущем, были применены методы предиктивной аналитики. Детальный анализ каждой уязвимости, включая оценки сообщества экспертов, предоставленные через OpenCVE, является ключевым аспектом для эффективного прогнозирования и предотвращения будущих угроз. Это позволило оценить их потенциальное влияние на будущее развитие уязвимостей ПО и разработать эффективные стратегии реагирования, адаптированные к постоянно меняющемуся цифровому ландшафту.

Динамика развития уязвимостей ПО

Современный ландшафт кибербезопасности характеризуется не только количеством угроз, но и их сложностью и воздействием. Был проведён анализ изменения рангов и оценок CWE с углублением в конкретные уязвимости, их описания, оценки CVSS (Common Vulnerability Scoring System), уровни угроз и другие связанные данные за период с 2020 по 2023 годы. Анализ основан на интеграции рангов и оценок CWE с детальным изучением связанных с ними CVE. Для каждой уязвимости были рассмотрены описания, оценки CVSS, уровни угрозы, типы уязвимостей, результаты проверок уровня угрозы, системные компоненты, механизмы эксплуатации и функциональность, что позволило создать многомерный портрет изменений в уязвимостях.

С 2020 по 2023 год происходили значимые изменения в рейтингах CWE, отражающие адаптацию сферы информационной безопасности к новым угрозам. Расширение векторов атак из-за проникновения новейших технологий и сетевых функций в повседневную деятельность приводит к трансформации и появлению новых угроз. Основываясь на анализе динамики CWE, видна прямая связь этих изменений с распространенными уязвимостями в ключевых системах и сервисах, таких как Jenkins Pipeline, XWiki Platform, Arduino Create Agent, Node.js, IBM Cognos Dashboards и многих других, которые являются ключевыми в разработке ПО, управлении проектами и интернет-вещей (рисунок 1). Это подчеркивает важность непрерывной оценки и обеспечения мер безопасности, чтобы минимизировать риски в корпоративных и облачных средах.

График демонстрирует динамику рангов для наиболее значимых CWE. Наблюдается рост приоритетности уязвимостей, что отражает сдвиги в фокусе кибербезопасности.

Качественный анализ изменения рангов CWE

CWE-22: уязвимости, связанные с ненадлежащей проверкой путей к файлам, продолжают представлять серьёзную угрозу для таких систем, как Jenkins Pipeline, XWiki Platform, Arduino Create Agent и Node.js. Эти системы играют ключевую роль в процессах разработки программного обеспечения, управления проектами и интернет-вещей, что делает их приоритетными целями для атак и подчёркивает необходимость их защиты.

CWE-287: уязвимости, связанные с недостаточной аутентификацией, выявленные в таких продуктах как IBM Cognos Dashboards, Red Hat Ceph Storage, SALESmanago и системах управления идентификацией от Pingidentity и Authentik, подтверждают их распространённость в корпоративных и облачных средах. На фоне возрас-

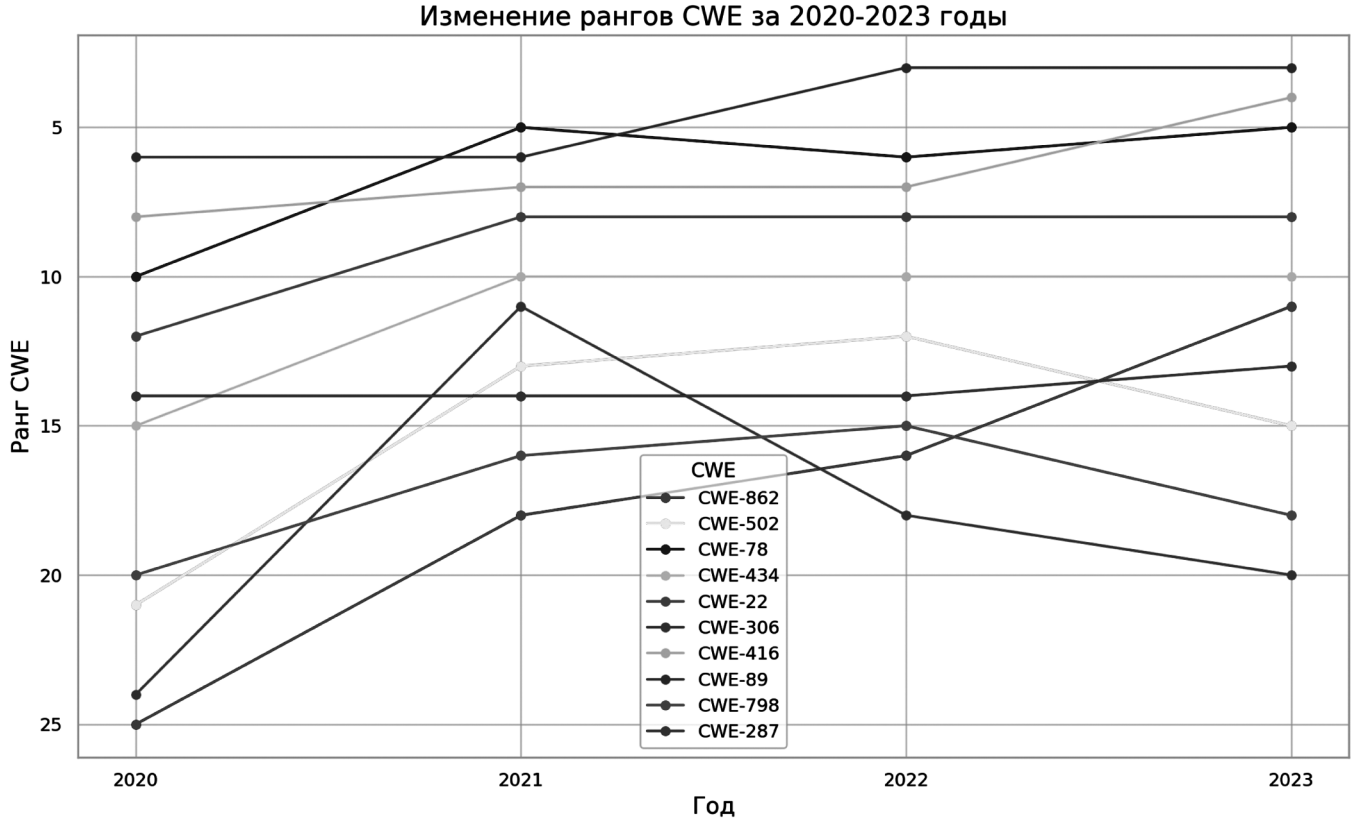

Рис. 1. Изменение рангов CWE за 2020–2023 годы

тающей зависимости от удалённого доступа и облачных технологий, проблемы с аутентификацией могут иметь серьезные последствия для безопасности данных и доступности услуг. Внимание к этому аспекту безопасности является критически важным, особенно в свете недавних инцидентов с Mitsubishi Electric, MISP и SICK, где атакующие могли обойти аутентификацию и получить доступ к чувствительным данным или системам управления.

CWE-306: отсутствие аутентификации для критически важных функций в продуктах, таких как Splunk Enterprise, SAUTER Controls Nova, PingFederate with PingID Radius PCV и IBM Sterling Partner Engagement Manager, отмечает существующие риски безопасности в корпоративных и облачных средах. Проблемы с аутентификацией в этих системах поднимают вопросы о защите критических операций, данных и инфраструктуры, поскольку отсутствие должных проверок может позволить неавторизованным лицам получить доступ к функционалу и чувствительной информации.

CWE-416: уязвимости типа Use After Free (Использование после освобождения), обнаруженные в таких продуктах, как Google Chrome, Linux Kernel, Android и macOS, подчеркивают важность защиты от сложных атак, способных привести к выполнению произвольного кода. Эти уязвимости могут быть использованы для повышения привилегий или удаленного выполнения кода, что делает их критическими угрозами для безопасности. Своевременное обновление и строгое управление памятью при разработке программного обеспечения должны быть обеспечены на высоком уровне.

CWE-434: уязвимость, обозначающая проблему «небезопасной загрузки файлов», является значительным и повторяющимся риском в разнообразных веб-приложениях и системах управления контентом (CMS). Как показывают данные по CVE, продукты такие как Pandora FMS и плагин Fancy Product Designer для WordPress столкнулись с серьезными уязвимостями, которые позволяют атакующим загружать произвольные файлы на сервер, что может привести к удаленному выполнению кода. Эти инциденты подчеркивают важность тщательного контроля за процессами загрузки файлов пользователями, включая проверку типов файлов и ограничения на доступ к загружаемым данным.

CWE-502: десериализация ненадежных данных выявляет значительные угрозы в широком спектре программных продуктов и систем, включая, но не ограничиваясь, такими как PredictAppak, PredictApp, Cacti, phpPgAdmin, и Splunk. Этот тип уязвимости также обнаружен в критических компонентах систем управления контентом и фреймворках для разработки, включая популярные инструменты, такие как Apache Struts и Jenkins. Риск связан с тем, что входные данные, контролируемые пользователем, могут быть десериализованы без должной проверки и очистки, что потенциально приводит к выполнению произвольного кода, злоупотреблению функциями приложений и в итоге к компрометации систем. Это подчеркивает необходимость строгих механизмов безопасности при работе с сериализованными данными и актуализирует необходимость своевременного обновления программного обеспечения для защиты от известных уязвимостей.

CWE-798: использование жестко закодированных учетных данных в продуктах таких компаний, как TIBCO Software, Siemens SICAM PAS и Cisco Emergency Responder, подчеркивает проблемы управления секретами и аутентификацией, которые остаются критически важными для программного обеспечения и промышленных контрольных систем. Эти уязвимости могут позволить злоумышленникам получить несанкционированный доступ и возможность выполнения произвольного кода, что усиливает необходимость своевременного обнаружения и устранения подобных уязвимостей в целях обеспечения безопасности.

CWE-862: Отсутствие проверки разрешений в различных компонентах, таких как системы управления доступом Boschrexroth HMI Web Panel, платформы Android от Google, плагины для Jenkins и сервисы от Palantir, подчеркивает риски безопасности, связанные с несанкционированным доступом и возможными привилегированными действиями на устройствах и системах. Это может привести к локальной и сетевой эскалации привилегий, утечке информации и другим видам атак, что делает проверки разрешений важной составляющей защиты информации.

CWE-89: Уязвимости SQL-инъекций, обнаруженные в ряде плагинов WordPress и других веб-приложений, таких как Demonisblack demon image annotation, Nucleus_genius Quasar form free, и Daniel Söderström / Sidney van de Stouwe Subscribe to Category, а также в системах, включая Avirtum ImageLinks и IT Path Solutions Contact Form to Any API, подчеркивают важность правильной санитизации пользовательского ввода и защиты от внедрения стороннего кода в SQL-запросы. Это критическое условие безопасности для веб-приложений, поскольку оно может привести к несанкционированному доступу к базам данных и потенциальной утечке конфиденциальной информации.

Почему уязвимости ПО остаются проблемой

Уязвимости, отнесенные к категориям CWE, продолжают быть значимыми и становятся всё более распространёнными по причине различных факторов.

CWE-22 (Path Traversal):
— Рост сложности систем увеличивает риск внедрения уязвимостей, связанных с обработкой путей файлов.
— Расширение векторов атак происходит из-за внедрения новых технологий.
— Неуловимость ошибок в коде, особенно в больших и сложных кодовых базах.

CWE-287 (Improper Authentication):
— Увеличение удаленного доступа и облачных технологий увеличивает зависимость от надежной аутентификации.
— Сложность разработки и поддержки аутентификационных механизмов, особенно при интеграции с разными системами.

CWE-306 (Missing Authentication for Critical Function):
— Увеличение числа критических систем, подключенных к Интернету.
— Сложность обеспечения удобства использования при сохранении безопасности.

CWE-416 (Use After Free):
— Сложность управления памятью в программировании на низком уровне.
— Продолжающееся использование устаревших технологий.

CWE-434 (Unrestricted Upload of File with Dangerous Type):
— Рост числа и функциональности веб-приложений.
— Техническая сложность надежного определения и блокирования потенциально опасного контента.

CWE-502 (Deserialization of Untrusted Data):
— Распространенность сериализации данных для передачи между системами.
— Сложность безопасной обработки сериализованных данных.

CWE-798 (Use of Hard-coded Credentials):
— Простота разработки и отладки с использованием жёстко закодированных учетных данных.
— Недостаток осведомленности о рисках безопасности.

CWE-862 (Missing Authorization):
— Сложность управления доступом в сложных системах.
— Расширение функциональности систем управления доступом.

CWE-89 (SQL Injection):
— Распространенность SQL-баз данных в веб-приложениях.
— Проблемы с эффективной защитой от SQL-инъекций.

Изменение рангов CWE

Анализ рангов общих слабых мест в ПО (по CWE) за период с 2020 по 2023 годы выявил важные тенденции и изменения в ландшафте уязвимостей, которые затрагивают различные отрасли и продукты. Ниже приведены ключевые результаты.

Веб-приложения и Платформы: такие уязвимости как CWE-22 и CWE-89, часто встречаются в веб-приложениях и платформах. Они продолжают быть высокоприоритетными из-за их распространенности и потенциального влияния на конфиденциальность, целостность и доступность данных.

Корпоративные системы и облачные решения: CWE, связанные с аутентификацией и авторизацией, такие как CWE-287 и CWE-306, были идентифицированы в корпоративных решениях. Это подчеркивает уязвимость облачных и корпоративных сред в условиях растущей цифровизации бизнес-процессов.

Браузеры и популярное ПО: уязвимость CWE-416 в Google Chrome и других распространенных программах показывает, что широко используемое ПО остается ключевой целью для злоумышленников, что требует постоянного внимания и обновлений безопасности.

Системы управления контентом (CMS): такие CWE, как CWE-434, обнаруженные в Fancy Product Designer WordPress и Pandora FMS, отражают риски, связанные с расширением функционала CMS через плагины и добавление пользовательских возможностей.

Разработка ПО и фреймворки: уязвимость CWE-502 в Apache Struts и Jenkins указывает на важность защиты приложений на этапе разработки, особенно в отношении безопасной обработки входных данных.

Промышленные и инфраструктурные системы: CWE-798 в продуктах TIBCO Software и Siemens демонстрирует необходимость улучшения практик управления учетными данными в критически важных системах.

Эти результаты подчеркивают необходимость сфокусированного внимания на уязвимостях, которые могут иметь значительные последствия для широкого спектра отраслей и приложений. В целом, они отражают важность обеспечения безопасности в эпоху цифровой трансформации и необходимость адаптации к постоянно меняющимся угрозам в сфере информационных технологий.

Прогнозирование тенденций в области уязвимостей ПО

Прогнозирование тенденций в области уязвимостей программного обеспечения может быть сложной задачей из-за множества переменных, включая изменения в технологических стеках, методах разработки и глобальных угрозах безопасности. Однако, анализируя текущие данные и тенденции в индустрии безопасности, можно предположить, что следующие CWE могут сохранить своё лидерство:

— CWE-79: учитывая растущую сложность веб-приложений, XSS остается важной угрозой.
— CWE-20 и CWE-80: как основа многих других видов атак, неправильная проверка входных данных, вероятно, останется проблемой.
— CWE-200 и CWE-311 (Information Exposure): с ростом данных и требований к конфиденциальности, уязвимости, приводящие к утечкам данных, могут стать ещё более значимыми.

CWE, которые могут выйти на первый план:

— CWE-400 и CWE-776: DoS-атаки становятся более изощрёнными.
— CWE-303 и CWE-287: сложность аутентификации может привести к новым уязвимостям.
— CWE-668 и CWE-319: с ростом использования микросервисов и облачных технологий, нарушение доверительных границ может стать более актуальным.

Новые или увеличивающиеся CWE.

Облачные технологии и контейнеризация:

— CWE-89, CWE-12 и CWE-122: неправильная проверка ввода может привести к серьезным уязвимостям в облачных приложениях, таким как SQL инъекции или атаки переполнения буфера.
— CWE-331 и CWE-337: неспособность генерировать и проверять криптографические значения в облачных сервисах может подвергнуть риск целостности и конфиденциальности данных.
— CWE-276: неправильно заданные разрешения по умолчанию могут дать злоумышленникам неожиданныйдоступкоблачнымресурсамилиданным.
— CWE-295: недостаточная проверка сертификатов может привести к принятию поддельных сертификатов, что угрожает безопасности шифрованных соединений.
— CWE-749: использование опасных функций может подвергать риск безопасности контейнеризированных приложений, которые полагаются на строгую изоляцию.
— CWE-400: утечка ресурсов в облачных средах может привести к перегрузке системы и снижению производительности.
— CWE-710: неправильная реализация контроля потока может нарушить предсказуемость и надежность облачных операций.
— CWE-284 и CWE-94: опасный вызов функции без проверки в облачных приложениях может привести к выполнению произвольного кода.

Искусственный интеллект и машинное обучение:

— CWE-457: использование неинициализированной памяти может вызвать непредсказуемое поведение моделей и алгоритмов AI/ML.
— CWE-120 и CWE-122: переполнение буфера может повлиять на целостность данных, что является критическим для алгоритмов обработки данных в AI/ML.
— CWE-276 и CWE-284: неправильное назначение разрешений может позволить несанкционированный доступ к данным и моделям AI/ML.
— CWE-704: некорректное преобразование типов данных может привести к ошибочным вычислениям в алгоритмах машинного обучения.
— CWE-298: несоответствие в разделении ответственности может привести к сложностям в управлении зависимостями и модулями AI/ML.
— CWE-391: ошибки обработки ошибок могут вызвать непредвиденные сбои в системах AI/ML, что может привести к неправильным результатам.

Влияние глобальных событий.

Геополитические напряженности и кибервойны могут привести к росту уязвимостей, связанных с кибершпионажем и саботажем:

— CWE-284: неправильное управление доступом обеспечивает возможность несанкционированного удалённого выполнения кода, что может использоваться для кибершпионажа.
— CWE-77: уязвимости внедрения команд позволяют злоумышленникам выполнять команды на целевой системе, что может способствовать саботажу.
— CWE-598: утечка информации через URL может выдать конфиденциальную информацию, что полезно для разведывательной деятельности.
— CWE-918: Server-Side Request Forgery (SSRF) позволяет атакующему взаимодействовать с внутренней инфраструктурой системы, что может привести к удалённому саботажу.
— CWE-22: небезопасный прямой доступ к файлам может облегчить несанкционированный доступ к файлам системы.
— CWE-937: использование компонентов с известными уязвимостями — создаёт риски кибершпионажа и саботажа, особенно если злоумышленники эксплуатируют неисправленные уязвимости.
— CWE-94: уязвимости удаленного включения файлов могут привести к удалённому выполнению

произвольного кода, что является существенным риском при киберконфликтах.

Важно отметить, что эффективность средств защиты и осведомлённость разработчиков могут сыграть решающую роль в изменении тенденций. Компании и сообщества, активно внедряющие лучшие практики безопасности и своевременно обновляющие программное обеспечение, могут повлиять на снижение частоты и серьёзности определённых CWE.

Визуализация анализа данных

Визуализация данных CWE позволяет наглядно представить распределение и частоту различных типов уязвимостей. Переходя от теоретического описания к практическому анализу, можно визуализировать вышеописанную классификацию уязвимостей, чтобы более наглядно представить распределение и частоту различных типов уязвимостей (рисунок 2, рисунок 3). Эта визуализация подчеркивает наиболее критические аспекты безопасности, которые были выявлены в данных CWE за последние годы.

На диаграммах представлено распределение уязвимостей, в т. ч. наиболее часто эксплуатируемых, классифицированных по ключевым параметрам: типу уязвимости, уровню угрозы, компоненту системы, механизму эксплойта и функциональным последствиям.

Представленная визуализация и анализ подчеркивают необходимость постоянного мониторинга уязвимостей ПО и принятия активных мер по их устранению и предотвращению. Также они указывают на области, требующие особого внимания при проектировании и тестировании программного обеспечения.

На основании проведенного анализа уязвимостей ПО по CWE за период с 2020 по 2023 годы, можно выделить следующие ключевые рекомендации:

1. *Придерживаться лучших практик безопасности*: важно внедрять и соблюдать лучшие практики безопасности на всех этапах жизненного цикла разработки ПО. Это включает в себя как раннее обнаружение уязвимостей, так и их устранение до выпуска продукта.

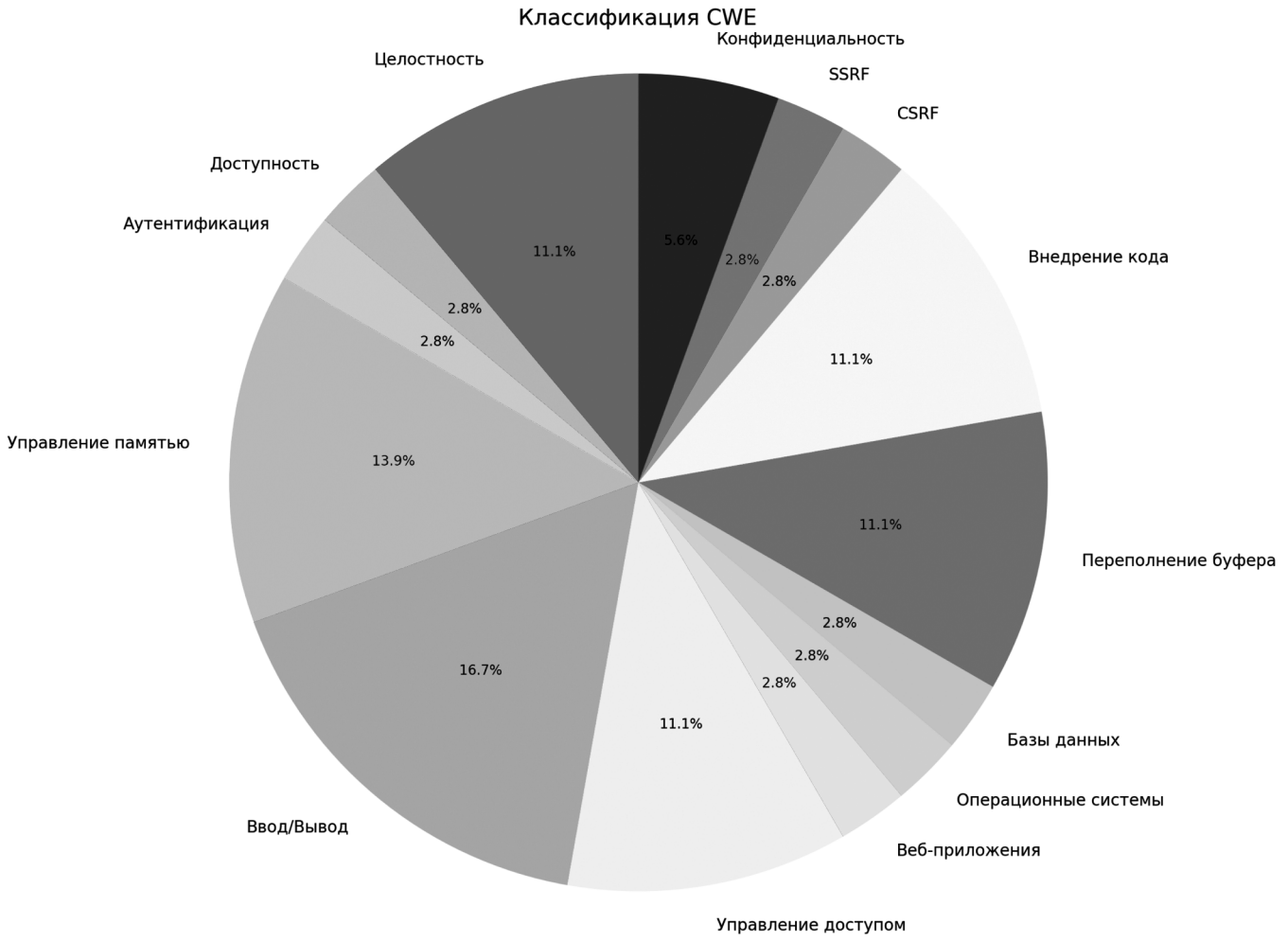

Рис. 2. Распределение уязвимостей ПО по категориям

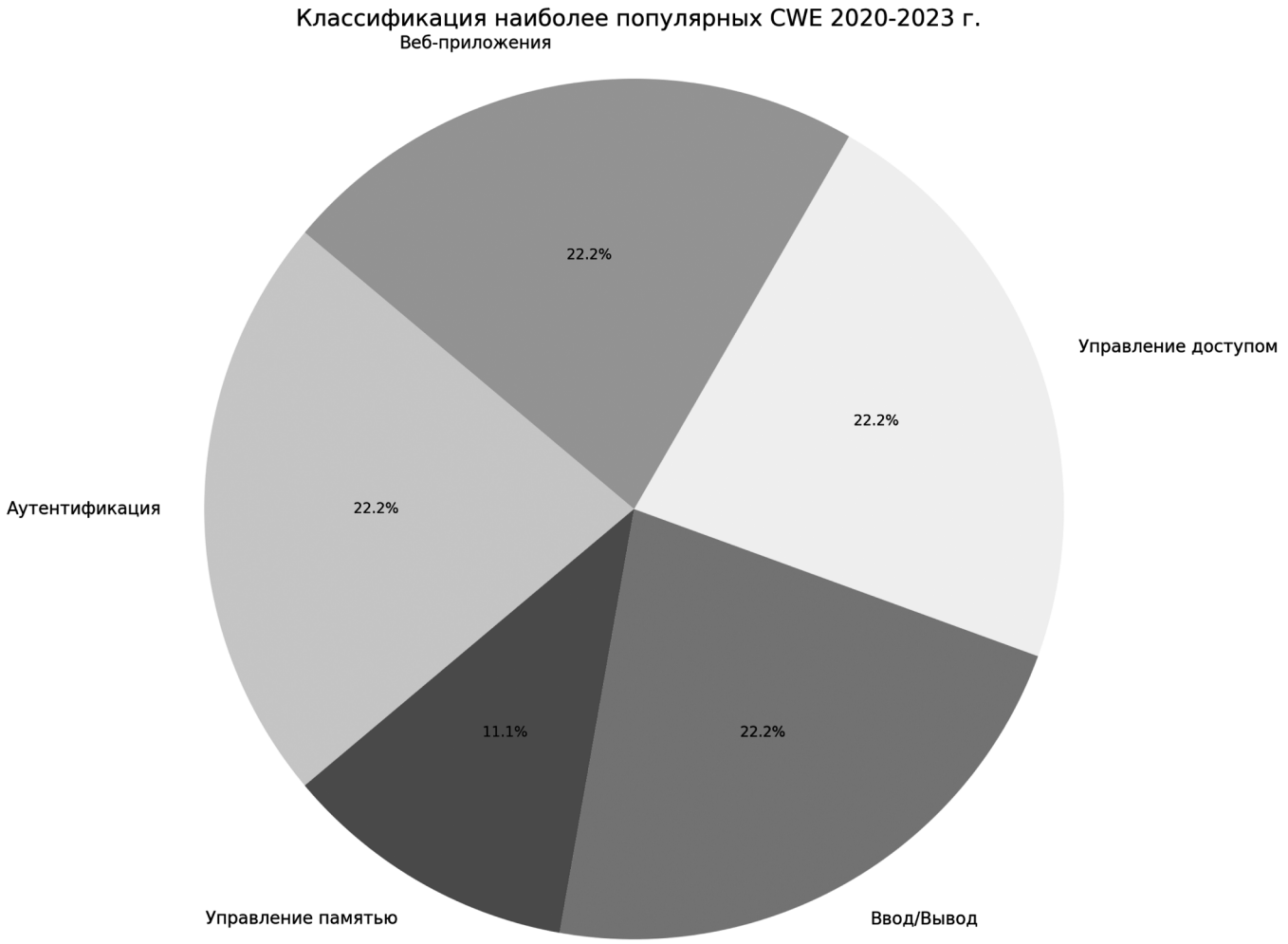

Рис. 3. Наиболее часто эксплуатируемые уязвимости CWE за 2020–2023 годы

2. *Обучать и повышать квалификацию разработчиков*: постоянное обучение и повышение квалификации разработчиков в области безопасного кодирования является ключевым для предотвращения внедрения новых уязвимостей в программное обеспечение.
3. *Инвестировать в автоматизированное тестирование и анализ кода*: рекомендуется инвестировать в инструменты и технологии для автоматизированного тестирования и анализа кода, что позволит обнаруживать и устранять уязвимости, тем самым повышать уровень безопасности разработанных систем.
4. *Разрабатывать и внедрять усовершенствованные системы аутентификации и авторизации*: учитывая значительное влияние уязвимостей, связанных с аутентификацией и управлением доступом, особое внимание следует уделить разработке и внедрению усовершенствованных систем аутентификации и авторизации.

Эти рекомендации направлены на усиление общей безопасности программного обеспечения и снижение рисков, связанных с эксплуатацией уязвимостей. Они также способствуют повышению уровня осведомленности и компетенций в области кибербезопасности среди профессионалов, занятых в разработке ПО.

Заключение

Проведённое исследование показало, что сфера кибербезопасности постоянно развивается, и организациям необходимо быть готовыми к постоянному обновлению знаний и технологий для защиты своих систем. По мере развития технологий следует ожидать появления новых типов уязвимостей. Это требует от организаций гибкости в адаптации к новым угрозам и развитии методов защиты. Особое внимание следует уделить развитию машинного обучения, технологиям искусственного интеллекта и облачных технологий. Важность непрерывного обучения, адаптации и применения комплексного подхода к безопасности ПО не может быть переоценена. В свете выявленных тенденций организации должны сосредоточить свои усилия на разработке эффективных стратегий кибербезопасности, которые способны адаптироваться к постоянно меняющемуся ландшафту угроз.

ЛИТЕРАТУРА

1. Common Weakness Enumeration [Электронный ресурс]. — URL: https://cwe.mitre.org/index.html (дата обращения: 14.03.2024).
2. OpenCVE [Электронный ресурс]. — URL: https://www.opencve.io (дата обращения: 14.03.2024).
3. 2020 CWE Top 25 Most Dangerous Software Weaknesses [Электронный ресурс]. — URL: https://cwe.mitre.org/top25/archive/2020/ 2020_cwe_top25.html (дата обращения: 14.03.2024).
4. 2021 CWE Top 25 Most Dangerous Software Weaknesses [Электронный ресурс]. — URL: https://cwe.mitre.org/top25/archive/2021/ 2021_cwe_top25.html (дата обращения: 14.03.2024).
5. 2022 CWE Top 25 Most Dangerous Software Weaknesses [Электронный ресурс]. — URL: https://cwe.mitre.org/top25/archive/2022/ 2022_cwe_top25.html (дата обращения: 14.03.2024).
6. 2023 CWE Top 25 Most Dangerous Software Weaknesses [Электронный ресурс]. — URL: https://cwe.mitre.org/top25/archive/2023/ 2023_top25_list.html (дата обращения: 14.03.2024).