ВАЖНАЯ ВЕХА В БЕЗОПАСНОСТИ ОТКРЫТОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Марков А.С.[1]

Уважаемые читатели!

Поздравляем всех с наступившим 2023 годом!

Традиционно многие игроки рынка информационной безопасности представили новогодние аналитические отчеты и прогнозы[2]. Эта аналитика еще раз подтвердила объективные вызовы в сфере кибербезопасности как глобального характера в виде озабоченности, связанной с внедрением прорывных технологий искусственного интеллекта и квантовых вычислений, так и касаемых динамики архитектур, угроз и мер защиты. Что касается Российской Федерации, то, по известным причинам, перед нами стоят задачи обеспечения технологического суверенитета страны при усилении наступающей составляющей информационной безопасности. В этом плане в стране значительно активизировались обсуждения применения программного обеспечения с открытым исходным кодом, особенно в условиях новых угроз, на что, собственно, и хотелось бы отдельно обратить внимание читателей журнала.

DOI:10.21681/2311-3456-2023-1-2-12

Исторический ракурс от OSS к OSS 2.0

В этом году, 27 сентября, прогрессивное человечество будет отмечать 40 лет революционной парадигме, а 3 февраля — 25 лет дефиниции программного обеспечения с открытым исходным кодом (англ.: open source software, OSS, free open source software, FOSS), что позволяет нам подвести некоторые важные итоги, в том числе имеющие актуальный характер для нашей страны.

В глоссариях ГОСТ, ISO, IEC, NIST и DoD программное обеспечение с открытым исходным кодом (ОПО) определяется как программное обеспечение с доступным для использования исходным кодом в соответствии с некоторой «свободной[3]» лицензией. В области информационной безопасности данное определение нельзя считать исчерпывающим, так как оно скрывает потенциал сообщества энтузиастов-программистов, стоящего за ОПО и обеспечивающего его создание и поддержку на протяжении всего его жизненного цикла. Поэтому неформально ОПО можно представить как доступное, совместно используемое программное обеспечение с исходным кодом, «свободной» лицензией по его использованию, а также комьюнити (организации), обладающим некоторым уровнем зрелости. С точки зрения программной безопасности важно различать готовый продукт и готовые компоненты (библиотеки, фреймворки).

В геополитическом смысле ОПО для нашей страны имеет безусловное архиважное значение, так как дает доступ к современным технологиям, в том числе к программным средствам защиты информации с открытым кодом[4]. Что касается безопасности кода, то имеются дискуссионные моменты. К примеру, в на-

3 The Open Source Definition. OSI. URL: https://opensource.org/osd

4 Open Source Security Index. URL: https://opensourcesecurityindex.io/

1 Марков Алексей Сергеевич, доктор технических наук, CEH, CISSP, главный редактор журнала «Вопросы кибербезопасности», Москва, Россия. E-mail: editor@cyberrus.com

2 ИБ-прогнозы на 2023 г. URL: https://t.me/EchelonEyes/1175

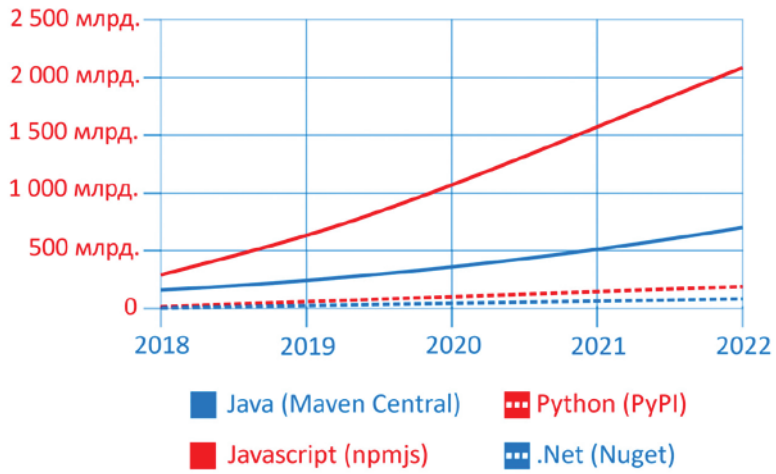
Рис. 1. Соотношение проблемы безопасности открытого кода и проблемы безопасности цепей поставки

Рис. 2. Условные плюсы и минусы открытого программного обеспечения

циональном стандарте ГОСТ Р 54593-2011 зафиксировано, что ОПО – это безопасная и надежная программная платформа, обеспечивающая раннее обнаружение дефектов и быстрое их исправление и т.д. В противоположность этому сообщества разработчиков программ чуть больше года назад объявили о «кризисе отрытого кода» [1-11], и даже уязвимостью года назвали классическую уязвимость ОПО (log4shell)[5]!

Технически ОПО отличается от закрытого программного обеспечения обязательным наличием исходных текстов программ, что позволяет использовать статические анализаторы качества, безопасности и инвентаризации кода, а также обеспечивать прозрачность расследования при инцидентах и т.п. В качестве классического недостатка современного ОПО отмечают проблемы заимствования и наследования компонентов кода, создаваемого различными комьюнити, что делает проблему безопасности ОПО конгруэнтной проблеме безопасности цепей поставок [12]. Так, в 2022 г. указанный фактор был самым значимым: согласно исследованию компании Sonatype [2], 6 из каждых 7 уязвимостей в проектах ОПО возникло из-за переходных зависимостей (рис. 1). Последнее означа-

5 PT: Какие уязвимости будут главными угрозами в 2023 году. URL: https://securitymedia.org/news/positive-technologies-kakie-uyazvimosti-budut-glavnymi-ugrozami-v-2023-godu.html



Источник: Sonatype

Рис. 3. Годовые объемы загрузки пакетов открытого программного обеспечения

ет, что проявление уязвимой зависимости может быть очень масштабным. Например, уязвимость в OpenSSL (по сути, переполнение буфера) привела к компрометации почти каждого пятого веб-сервера в мире. Ситуация осложняется тем, что отмечается тенденция роста зависимостей в современных продуктах. Например, число зависимостей в Java-проектах только за последний год выросло в десять раз!

Надо понимать, что организационные вопросы обеспечения безопасности программного кода на всем жизненном цикле принципиально определяются зрелостью комьюнити и могут составлять проблемы, например, при поддержке программного продукта в реальном времени. Некоторые плюсы и минусы ОПО приведены на рис. 2.

Возьмем на себя смелость утверждать, что мир находится в трансформации от свободной «коммунистической» парадигмы ОПО к геополитической прагматичной парадигме ОПО 2.0. Этому свидетельствуют следующие моменты:

1. **Зависимость современных информационных технологий от ОПО**. Так, технологии ОПО фактически перестали быть отдельной линейкой развития производства программ и интегрировались в жизненный цикл проприетарного коммерческого программного обеспечения и программного обеспечения, финансируемого государством.

2. **Государственное регулирование ОПО**. Прошлый год испытал взрыв публикаций законодательных и нормативных актов, посвященных ОПО.

3. **Кризис доверия к безопасности ОПО в части устойчивости и безопасности**. Классические факторы ОПО (зависимость от наследуемых компонент и распределенные сообщества разработчиков) стали причиной масштабных сбоев и атак на защищенные информационные системы, а безопасность цепей поставок стала синонимом безопасности ОПО.

Это свидетельствует, что исследования в данной сфере остаются весьма востребованными, и в данном обсуждении мы рассмотрим названные особенности ОПО 2.0, затронем новые факторы информационной безопасности и наметим пути дальнейших изысканий.

В заключение подраздела следует отметить интерес к проблеме со стороны научного сообщества. Так, по оценкам [13] за последние 5 лет тематике посвящено 1025 публикаций, около 180 из них признаны представительными. Можно сделать ремарку, что в состав последних вошла одна российская научная публикация [14].

1. Феномен зависимости от открытого программного обеспечения

В настоящее время четко наблюдается экспоненциальный рост использования ОПО, очевидно смещение рынка программных систем в область ОПО и интеграция ОПО в коммерческие и государственные проекты.

Например, по оценкам компании Sonatype, в 2022 году только по четырём популярным экосистемам (Java, JavaScript, Python, .NET) количество загружаемых и интегрируемых в программное обеспечение зависимостей с открытым исходным кодом выросло более чем на треть, общий объем загрузок пакетов превысил 3 триллиона (рис. 3), создано более

Таблица 1

Законодательные и нормативно-правовые акты США, релевантные тематике открытого программного обеспечения

Год	Название
	Указы президента США
2021	Executive Order on Improving the Nation's Cybersecurity, EO 14028.
	Концептуальные документы
2022	Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. *Executive Office of The President. OMB.*
	Федеральные законы
2021	DHS Software Supply Chain Risk Management Act
2022	Securing Open Source Act
2021	Supply Chain Security Training Act
	НПА органов исполнительной власти
2022	Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure. SEC
2022	Enhancing the Security of the Software Supply Chain through Secure Software Development Practices. *OMB*
2021	SBOM Proof of Concept. V.2.0. *NTIA*
2022	Securing the Software Supply Chain: Recommended Practices Guide for Developers. *NSA, CISA, ODNI*
	Нормативные документы и специальные публикации
2022	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. NIST SP 800-161r1. *NIST*
2021	Defending Against Software Supply Chain Attacks. *NIST, CISA*
2021	Guidelines on Minimum Standards for Developer Verification of Software. NISTIR 8397. *NIST*
2022	Secure Software Development Framework. V.1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. NIST SP 800-218. *NIST*
2022	Software Supply Chain Security Guidance Under Executive Order (EO) 14028. *NIST*
2021	Software Supply Chain Security Guidance. *NIST*

3.3 млрд проектов и 47 млрд версий проектов. Забегая вперед, можно добавить, что вместе с триллионами пакетов было загружено почти 15 млрд зависимых уязвимых компонентов кода.

По оценкам Open Source Initiative, за прошлый год 77% организаций в США увеличили использование ОПО. При этом, кроме систем производства программ зафиксирован значительный рост (более чем на треть) использования открытых баз данных, ОС, репозиториев Git, фреймворков AI/ML и др. Отчасти это связано с ростом популярности технологий AI/ML, технологий обработки Big Data, DevOps и других современных технологий [11].

Согласно данным испытательной лаборатории НПО «Эшелон», в период 2019-2022гг. в рамках проверки 860 проектов 97% программных средств защиты информации и 74% специального ПО имели в своем составе компоненты ОПО. Эксперты полагают, что 2/3 программного кода современных защищенных операционных систем уже состоят из компонентов ОПО.

Вопросы зависимости уровня качества, надежности и безопасности современных программных систем от компонентов ОПО мы затронем ниже.

2. Государственное регулирование степени открытости открытого программного обеспечения

Прошедшая пара лет ознаменовала совершенно новый этап государственного регулирования области «открытости» и безопасности ОПО. Наиболее примечательным можно назвать американский законопроект 2022 года «Акт о защите ОПО» (Securing Open Source Software Act, SOSSA), который ожидается к утверждению в текущем году. Законопроект фактически устанавливает американскому Агентству кибербезопасности и безопасности инфраструктуры (CISA) стать координационным центром в США в вопросах безопасности ОПО на всех этапах его жизненного цикла. Агентству поручена концепция оценки риска компонентов ОПО. В совокупности с другими федеральными структурами планируется создать так называемые офисы (центры компетенции и взаимодействия с комьюнити ОПО) программ с открытым исходным кодом — OSPO и даже разработать обязанности главных информационных директоров, касающиеся безопасности ОПО. Самое интересное, что законопроект предусматривает внесение поправки в Закон о национальной безопасности 2002 года, чтобы официально признать ОПО частью **критической инфраструктуры страны**. Об амбициях и решительности американско-

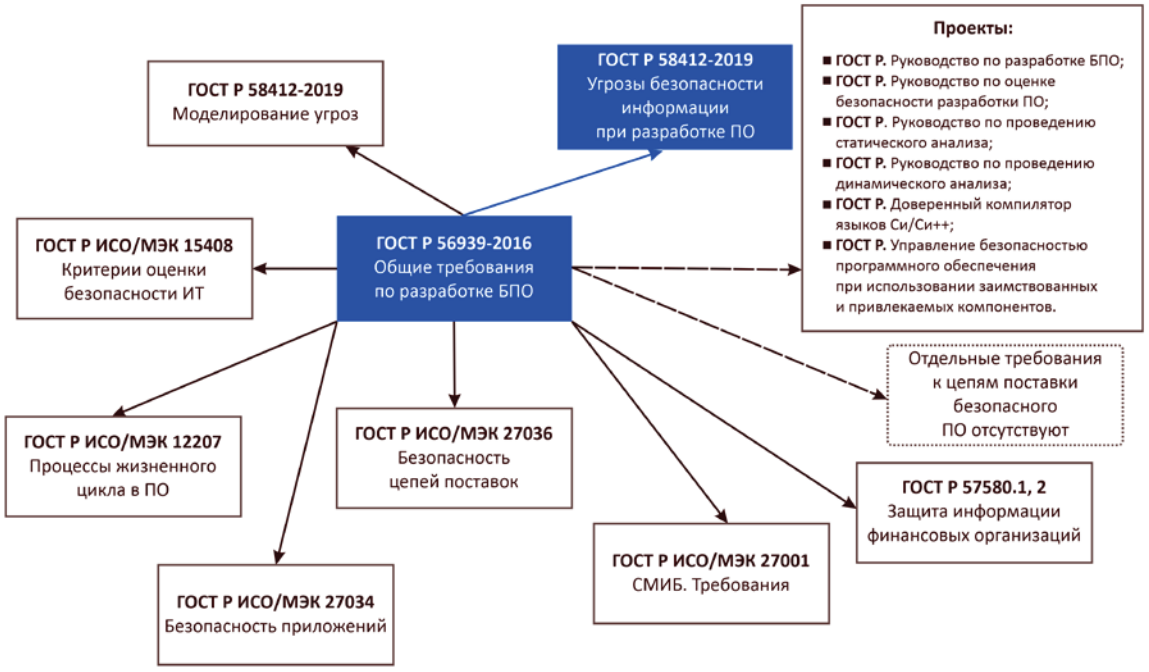


Рис. 4. Гармонизация стандартов по линии разработки безопасных программ

го госрегулирования тематики ОПО можно судить по табл. 1 (не претендующей на полноту).

Можно добавить, что 2021–2022 годы были знаменательны в плане озабоченности безопасностью ОПО для большинства сателлитов США, а именно: НАТО, ЕС, Великобритании и даже «Океанской четверки» (США, Австралия, Индия, Япония), — любознательный читатель легко может познакомиться самостоятельно.

Что касается России, то востребованность ОПО назрела, по известным причинам, очень давно, и правительство делало ряд важных шагов по развитию тематики [15]. В настоящее время государственное регулирование ОПО в стадии развития (особенно с учетом отказа от иностранного программного обеспечения на объектах КИИ РФ согласно Указу Президента РФ 2022 г. № 166). Перечислим последние основные инициативы (в первую очередь со стороны Минцифры России, ФСБ России, ФСТЭК России и др.), а именно:

- создание национального репозитория и формирование нормативной базы публикации открытого программного обеспечения (см. постановление Правительства РФ 2022 г. № 1804);
- исследование национальной базовой системной среды (ядра Linux[6]);
- оперативное реагирование со стороны регуляторов на атаки и уязвимости ОПО[7],[8].
- формирование требования к открытому программному обеспечению для его включения в реестр российского программного обеспечения,
- поддержка движения ОПО и др.

В стране с 2021 года заинтересованные стороны обсуждают проект «Стратегия развития программного обеспечения с открытым кодом в России»[9], но пока проект носит декларативный характер завтрашнего дня. Любознательный читатель может сравнить проект с проектом Концепции развития разработки и использования свободного программного обеспечения в РФ[10].

Можно посетовать на отсутствие национальных стандартов по линии безопасности ОПО и цепей поставок (рис. 4), в то же время последние все-таки както обозначены в ГОСТ Р 56939-2016 [12, 16]. Более того, новый тренд на разработку безопасных про-

6 ФСТЭК предложила бизнес-сообществу включиться в поиск уязвимостей Linux. URL: www.rbc.ru/newspaper/2021/10/19/6169b21e9a79470ef5987a76

7 Рекомендации по компенсации ИТ-рисков для компаний и организаций РФ в условиях санкционных ограничений. НКЦКИ, 2022. — ALRT-20220319.1.

8 Рекомендации по безопасной настройке операционных систем Linux. ФСТЭК России, 2022.

9 Стратегия развития программного обеспечения с открытым кодом в России до 2024 года. Проект. 2021. URL: https://d-russia.ru/wp-content/uploads/2021/10/proekt_strategii_opo_30_09_21.pdf

10 Концепции развития разработки и использования свободного программного обеспечения в РФ. Проект. V 3.0. 2008. URL: https://limited-ussvu.mil.ru/upload/site113/document_file/Koncepciya_razvitiya_i_ispolzovaniya_programmnogo_obespecheniya.pdf

грамм имеет целью именно снижение уровня уязвимости программных ресурсов и наследуемых компонентов на всем жизненном цикле.

3. Кризис доверия к безопасности открытого программного обеспечения

Объем колонки редактора имеет ограниченный объем, поэтому мы затронем лишь верхушку айсберга проблематики информационной безопасности ОПО: динамику и таксономии уязвимостей и атак, специфические атаки, практики и оценку соответствия.

Несмотря на концепцию «много глаз», компоненты ОПО остаются весьма уязвимыми [17], в первую очередь по причине критической структурной сложности программ и нечеткой обратной связи от пользователей. В качестве курьеза можно назвать недавно обнаруженную удалённо эксплуатируемую уязвимость в команде *ping* из состава OpenBSD, возраст которой превысил 25 лет[11]. Отметим следующие факторы безопасности современного ОПО:

- наличие актуальных уязвимых компонентов ОПО в текущий момент (до 8.4% [4]);
- наличие критических проектных ошибок (например, CVE-2021-44228, log4shell), способных привести к масштабным последствиям;
- взрывной рост атак, направленных на открытый исходный код в публичных репозиториях и атак на цепочку поставок (рис. 5).

По оценкам [9] почти каждая пятая уязвимость ОПО носит преднамеренный характер. Таким образом, можно привести общую классификацию ОПО по степени зависимости от внешних компонент и по степени преднамеренности:

- уязвимости, связанные с переходными (транзитивными) зависимостями, и другие (рис. 1);
- уязвимости, не идентифицированные как преднамеренные, программные закладки и злоупотребления в виде протестного программного обеспечения и блокировок (рис. 6).

Данная классификация позволяет легко понять, какие конкретные методы выявления дефектов и уязвимостей предпочтительны при анализе кода и тестировании программ.

Классическими представителями «непреднамеренных» уязвимостей является CVE-2014-0160, которая привела к компрометации около 18% веб-серверов в мире[12] и CVE-2021-44228, представляющая потенциальную опасность для 40% подсетей в мире[13].

Примером преднамеренной уязвимости является добавление вредоносной библиотеки в среду Python (CVE-2020-15523). Другим ярким примером внесения вредоносного кода служит атака на экосистему SolarWinds, скомпрометировавшая 18 000 клиентов компании и пр.

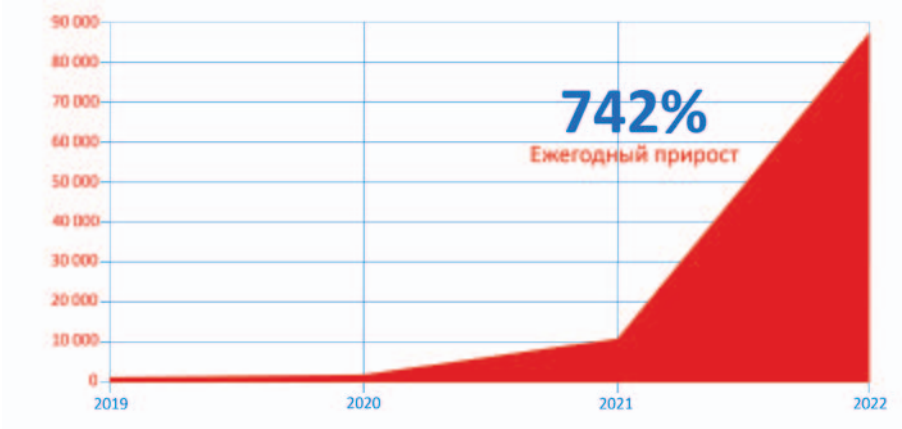
Протестное программное обеспечение относительно новый класс атак, который включает демонстрацию баннеров в описании репозитариев программ, запись политических призывов в журналы программ, демонстрацию политических баннеров при установке ОПО и деструктивные воздействия. Самым ярким примером протестного программного обеспечения явилась закладка CVE-2022-23812, когда автор пакета node-ipc внес обфусцированный код, который перезаписывает содержимое файлов на эмоджи-сердечки (♥) если код пакета был запущен с российского или белорусского сетевого адреса. Надо понимать, что протестное программное обеспечение (как и блокировка учетных записей GitHub российских компаний, находящихся под санкциями) носит вид злоупотребления этикой открытого и свободного программного обеспечения, так как деструктивный хактивизм не поддерживается множеством профессиональных комьюнити. В то же время масштаб кибератак против нашей страны, по мнению официальных лиц, носит беспрецедентный характер. Так, по сообщениям «Лаборатории Касперского», в феврале прошлого года было выявлено 100 вредоносных элементов в иностранном ОПО, а к июню количество закладок в ОПО увеличилось в 20 раз.

В целом, к специфическим атакам на ОПО относят атаки использования зависимостей (dependency confusion) и хактивизм (protestware). К первому классу относят атаки подмены пакета, внедрение вредоносного кода в пакет, внедрение вредоносного пакета с подобным именем или с опечатками (Combosquatting, Altering Word Order, Manipulating Word Separators, Typosquatting, Brandjacking и др.), а также атаки на систему производства программ. В качестве забавного примера любопытен эксперимент по подмене названия пакета, когда автор за возна-

11 Проверка утилиты ping в OpenBSD выявила ошибку, присутствующую с 1998 года. URL: www.opennet.ru/opennews/art.shtml?num=58299

12 Half a million widely trusted websites vulnerable to Heartbleed bug. URL: https://news.netcraft.com/archives/2014/04/08/half-a-million-widely-trusted-websites-vulnerable-to-heartbleed-bug.html

13 Leonid Grustniy. Log4Shell год спустя. URL: www.kaspersky.ru/blog/log4shell-still-active-2022/34362/



Источник: Sonatype

Рис. 5. Рост кибератак на цепочки поставок

Рис. 6. Классификация уязвимостей программ по степени преднамеренности

граждение продемонстрировал взлом 35 крупнейших компаний-разработчиков программ[14].

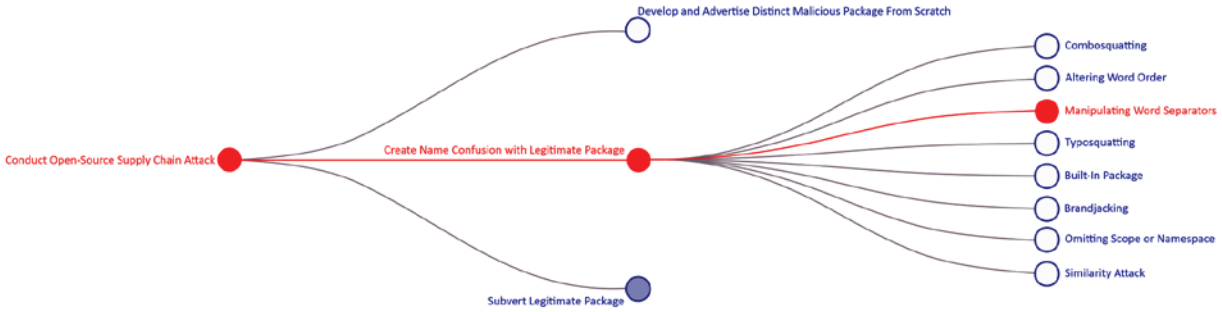
Что касается таксономий атак на ОПО, то в [2] рассматриваются 23 атаки, а в [13] – 107. На рис. 7 приведена интерактивная визуализация таксономии, представленной в репозитории SAP.

Отдельного упоминания заслуживает матрица Open Software Supply Chain Attack Reference (OSC&R), выполненная в виде «тактик, техник и процедур» (рис. 8).

Несмотря на кризис доверия, в мире проблема безопасности ОПО понимаема как со стороны научного сообщества, так и регуляторов индустрии информационной безопасности. Кроме таксономий угроз и атак, в литературе предлагается ряд организационно-технических мер защиты, например, в [8] приведены 10 рекомендаций, в [6] дан анализ 20 «хороших практик», в [13] приведены 33 контрмеры, в [13] – 113 проверок и т.д. Для наглядности в табл. 2 приведены первоочередные задачи, представленные в «Мобилизационном плане» Linux Foundation.

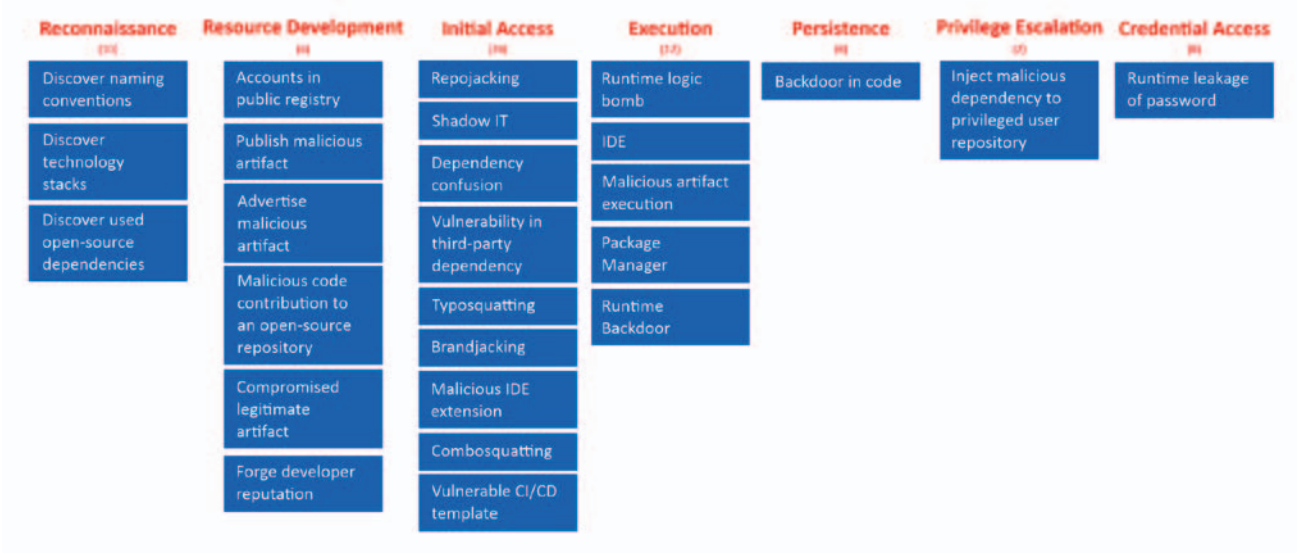
Что касается инструментария, то, конечно, выделяются специфические средства анализа компонентов и поддержки спецификаций зависимостей открытого

14 Birsan A. Dependency Confusion: How I Hacked into Apple, Microsoft and Dozens of Other Companies. URL: https://medium.com/@alex.birsan/dependency-confusion-4a5d60fec610



Источник: https://sap.github.io/risk-explorer-for-software-supply-chains

Рис. 7. Дерево атак на цепи поставок



Источник: https://pbom.dev

Рис. 8. Срез Open Software Security в OSC&R

кода — Software Composition Analysis / Open Source Analysis. Ряд отечественных компаний даже предлагают онлайн-сервисы сканирования пакетов ОПО на известные уязвимости[15]. Но надо понимать, что подобные средства являются лишь тривиальным компонентом современных комплексов статического и динамического анализа программ, например класса АК-ВС 3.

Оценка соответствия

Обзор проблемы безопасности ОПО был бы неполным, если бы мы не уделили внимание сертификации по требованиям безопасности информации, так как средства защиты информации в нашей стране имеют легитимный вид только при наличии сертификата соответствия от регулятора отрасли информационной безопасности (Минобороны России, ФСБ России, ФСТЭК России в рамках их компетенции). Как известно, в процессе сертификации ОПО может быть:

- собственно программным продуктом,
- сторонними (заимствованные, привлекаемые) компонентами,
- средой функционирования.

Напомним, что относительно требований к программному коду, проверяемому в обязательных или добровольных системах сертификации нашей страны, имеются требования доверия ФСТЭК России, профиль защиты ППО ФО (ОУД4+), задания по безопасности по ГОСТ ИСО/МЭК 15408, РД НДВ, а также проверка процессов по ГОСТ Р 56939. Указанные документы включают различные по содержанию и

15 Kaspersky Open Source Software Threats Data Feed. URL: www.kaspersky.ru/about/press-releases/2022_laboratoriya-kasperskogo-predstavila-pervyj-v-rossii-servis-dlya-vyyavleniya-zakladok-v-po-s-otkrytym-ishodnym-kodom

Таблица 2

Основные этапы и задачи обеспечения безопасности открытого кода

Этапы	Задачи
Обеспечение безопасности производства	Предоставление базового образования по разработке безопасного ОПО
	Создание публичной панели оценки рисков для лучших компонентов ОПО
	Ускорение внедрения цифровых подписей на релизах программного обеспечения
	Устранение первопричин многих уязвимостей путем замены небезопасных языков
Улучшение обнаружения и устранения уязвимостей	Создание команды быстрого реагирования (Open Source Security Incident Response Team)
	Ускорение обнаружения новых уязвимостей сопровождающими и экспертами с помощью передовых инструментов безопасности и экспертного руководства
	Проведение (раз в году) независимых обзоров кода (и любые необходимые работы по исправлению) наиболее важных компонентов ОПО
	Координирование обмена данными в масштабах отрасли для улучшения исследований, помогающих определить наиболее критичные компоненты ОПО
Сокращение времени отклика на исправления экосистемы	Улучшение инструментария инвентаризации зависимостей (SBOM) и обучение для стимулирования внедрения
	Усовершенствование наиболее важных систем сборки ОПО менеджеров пакетов и систем распространения с помощью лучших инструментов и передовых методов обеспечения безопасности цепочки поставок

Таблица 3

Особенности проверки открытого программного кода

Методы анализа и тестирования	Открытый код		Проприетарный код	
	Преимущество	Недостатки	Преимущество	Недостатки
Статический анализ	Обычно хорошо закомментированный и «чистый» код	**Обычно нет доступа к разработчику для разъяснения**	**Доступ к разработчикам для пояснения**	Из-за спешки может быть плохой некомментированный код и, как следствие, со множеством ошибок
Фаззинг	Большинство решений консольные и достаточно просто интегрируются	В случае сложности проекта необходимо эксперту ИЛ самостоятельно писать прослойку для фаззинга	**Разработчик берет на себя написание прослойки в случае необходимости**	Из-за того, что во многих компаниях разработка — это непрерывный процесс, то может возникнуть дефицит ресурсов для реализации прослойки
Пентест	Решения обычно открытые и, как следствие, уже есть наработки по ним на общих ресурсах	Сложно узнать некоторые глубинные технологии и, как следствие, меньше специфической информации, которая могла бы помочь	Полное описание продукта с доступом к инженеру, который может ответить на любой вопрос	Проблемы с пониманием старого кода, который писали, например, уволившиеся программисты
Динамический анализ		Сложность интеграции		Сложность интеграции

глубине процедуры анализа кода и тестирования программ. В табл. 3 показаны достоинства и недостатки базовых методов проверки безопасности программ (по мнению экспертов испытательной лаборатории НПО «Эшелон»).

Так как при сертификации в любом случае предоставляется исходных код, то разница по уровню безопасности открытого и проприетарного кода нивелируется и акцент смещается к уровню зрелости организации или общества разработчиков (рис. 9).

Заключение

Таким образом, можно констатировать, что мы становимся свидетелями новой итерации парадигмы

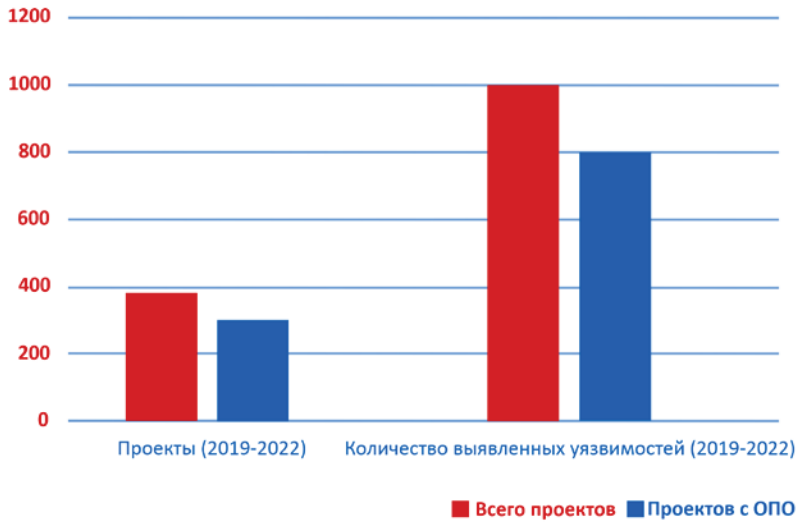


Рис. 9. Сравнение уязвимости проприетарного и открытого программного обеспечения

ОПО 2.0 (Open Source Software 2.0), которая, на наш взгляд, характеризуется глубокой интеграцией компонентов открытого кода с современными программными системами, государственным регулированием и новыми факторами информационной безопасности цепей поставки.

Отдельно следует отметить геополитическую значимость ОПО. И речь идет не только об использовании открытых стандартов и технологий в целях обмена (получения) знаний. В эпоху IV промышленной революции ОПО становится важным киберресурсом международного соперничества и противоборства, включающих гонку за установление собственных технических и нормативных стандартов, протоколов, систематик, языков, архитектур, моделей, датасетов, объединений сообществ и пр. Несмотря на этические декларации ОПО, все чаще видятся прагматические его аспекты, регулируемые государством. Не секрет, что в политических публикациях и даже отдельных доктринных документах западных стран прослеживается наступательных характер информационной безопасности. Можно встретить высказывания, что сам факт существования российского открытого кода уже представляет киберугрозу национальной безопасности США [18].

В то же время организационно-технические и технические аспекты безопасности ОПО понятны, идет совершенствование таксономий, создание методической базы и инструментария проверок ОПО, развитие технологий и средств защиты, их адаптация под новые архитектуры (облачные, микросервисные и пр.), внедрение прорывных технологий (AI/ML, Big Data), а также формирование сертификации специалистов по ОПО.

Что касается нашей страны, то, несмотря на математический потенциал, российские участники международных проектов с открытым исходным кодом пока довольствуются 6-9 местом в мире[16]. Однако налицо своевременная активность регуляторов, научных институтов, государственных корпораций и общественных объединений. Можно добавить, что положительный опыт российской сертификации средств защиты информации демонстрирует, что «кризис открытого кода» разрешим. Это вселяет уверенность в скорейшем решении поставленных в стране задач, и не только в плане обеспечения технологического суверенитета и технологической независимости, а и в создании самых передовых прикладных технологий в мире. Но, как говорится, дорогу осилит идущий!

Главный редактор
Certified Ethical Hacker (EC-Council),
Certified Information Systems Security Professional (ISC)2,
доктор технических наук

Алексей Марков

16 Численность профессиональных разработчиков по странам. URL: www.jetbrains.com/lp/devecosystem-2021/demographics/

Литература

1. Behlendorf B. (foreword) and etc. OpenSSF 2022 Annual Report. The Open Source Security Foundation, 2022, 38 p.
2. Carter H. (foreword). 2022 State Software Supply Chain. The 8th Annual State of the Software Supply Chain report. Sonatype, 2022. URL: www.sonatype.com/state-of-the-software-supply-chain/.
3. Hendrick S. and Mckeay M. Addressing Cybersecurity Challenges in Open Source Software. The Linux Foundation and Snyk, 2022. 35 p.
4. Mayhew B. and etc. 2021 State Software Supply Chain. The 7th Annual Report on Global Open Source Software Development. Sonatype, 2021, 40 p.
5. Milner E. and Kosef R. CIS Software Supply Chain Security Guide. Center of Internet Security, 2022, 66 p.
6. Open Source Software Security: A Research Summary. GSMA, 2020, 59 p.
7. State of Open: The UK in 2021 Phase Three the Values of Open. Open UK, 2021, 35 p. URL: https://openuk.uk/wp-content/uploads/2021/10/openuk-state-of-open_final-version.pdf.
8. The Open Source Software Security Mobilization Plan. Linux Foundation & OpenSSF, 2022. 51 p.
9. The State of Open Source Software. Octoverse-2020. GitHub, 2020. URL: https://octoverse.github.com/#securing-software.
10. 2022 Open Source Security and Risk Analysis Report. The 7th edition of OSSRA. Synopsys Cybersecurity Research Center, 2022, 24 p. URL: www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2022.pdf.
11. 2022 State of Open Source Report. OpenLogic, 2022. URL: www.openlogic.com/resources/2022-open-source-report.
12. Барабанов А.В., Марков А.С., Цирлов В.Л. О систематике информационной безопасности цепей поставки программного обеспечения // Безопасность информационных технологий. 2019. Т. 26, № 3. С. 68-79. DOI: 10.26583/bit.2019.3.06.
13. Ladisa P., Plate H., Martinez M. and Barais O. SoK: Taxonomy of Attacks on Open Source Software Supply Chains. Proceedings of the Symposium on Security and Privacy, San Francisco, USA, 2023, pp. 167-184. DOI: 10.1109/SP46215.2023.00010.
14. Barabanov A., Grishin M., Markov A., Tsirlov V. Current taxonomy of information security threats in software development life cycle. In: 2018 IEEE 12th International Conference Application of Information and Communication Technologies (AICT). 2018, pp. 356– 361. DOI: 10.1109/icaict.2018.8747065.
15. Калюжный К.А. Свободное программное обеспечение как системообразующий фактор информационной среды науки и общества: состояние и перспективы // Наука. Инновации. Образование. 2014. №16. С. 240-264.
16. Барабанов А.В., Марков А.С., Цирлов В.Л. 28 магических мер разработки безопасного программного обеспечения // Вопросы кибербезопасности. 2015. № 5 (13). С. 2-10. DOI: 10.21681/2311-3456-2015-5-2-10.
17. Шабалин Ю. Опасность компонент с открытым исходным кодом в цифрах на реальном проекте // Информационная безопасность. 2022. № 4. С. 42-43.
18. Aitel D. and etc. Russian Open Source Code. In: Russia's Cyber Operations: A Threat to American National Security. Margin Research, 2022, pp. 83-96.