ФИНТЕХ — РАДАР 04

№4 ИЮЛЬ 2023

ТЕХНОЛОГИЯ МЕСЯЦА -

DevSecOps

БЕЗОПАСНАЯ РАЗРАБОТКА И РЕШЕНИЯ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ

Безопасная разработка и решения с открытым кодом - два важнейших тренда российского ИТ, которые на первый взгляд друг с другом конфликтуют. В этом выпуске АФТ поясняет, как достичь синергии между трендами и обеспечить долгосрочное безопасное развитие корпоративных ИТ-решений.

ТАКЖЕ В ЭТОМ ВЫПУСКЕ

– Руководство по внедрению генеративного ИИ для ИТ-руководителей
– Оценка окупаемости инвестиций в ИИ
– Конфиденциальность и социальные аспекты метавселенной

ТЕХНОЛОГИЧЕСКИЙ БЕНЧМАРК: КАК ОЦЕНИТЬ ЭФФЕКТИВНОСТЬ РАСХОДОВ НА ИТ?

Ассоциация ФинТех проводит пилотный проект по **технологическому бенчмаркингу**: оценка эффективности расходов на ИТ-функцию. Данное исследование дает уникальную аналитику по показателям эффективности ИТ-функций для финансовых компаний с учетом данных российского и международного рынка (включая Gartner и др.). Исследование поможет разработать рекомендации для формирования ИТ-стратегии компаний.

Сбор, анализ и дальнейшая интерпретация данных осуществляется **строго в защищенном периметре Ассоциации ФинТех**. Результаты персональных отчетов будут доступны конкретной компании по запросу, в которых **данные других респондентов будут представлены в агрегированной (обезличенной) форме.**

ПОДХОД К ПРОВЕДЕНИЮ ИССЛЕДОВАНИЯ

Исследование нацелено в первую очередь на **компании финтеха России**: банки, страховые компании и другие организации сектора, но в дальнейшем может быть масштабировано и на другие отрасли. В первой волне примут участие члены, ассоциированные члены и партнеры Ассоциации ФинТех.

Период исследования: **август-октябрь 2023 г.**

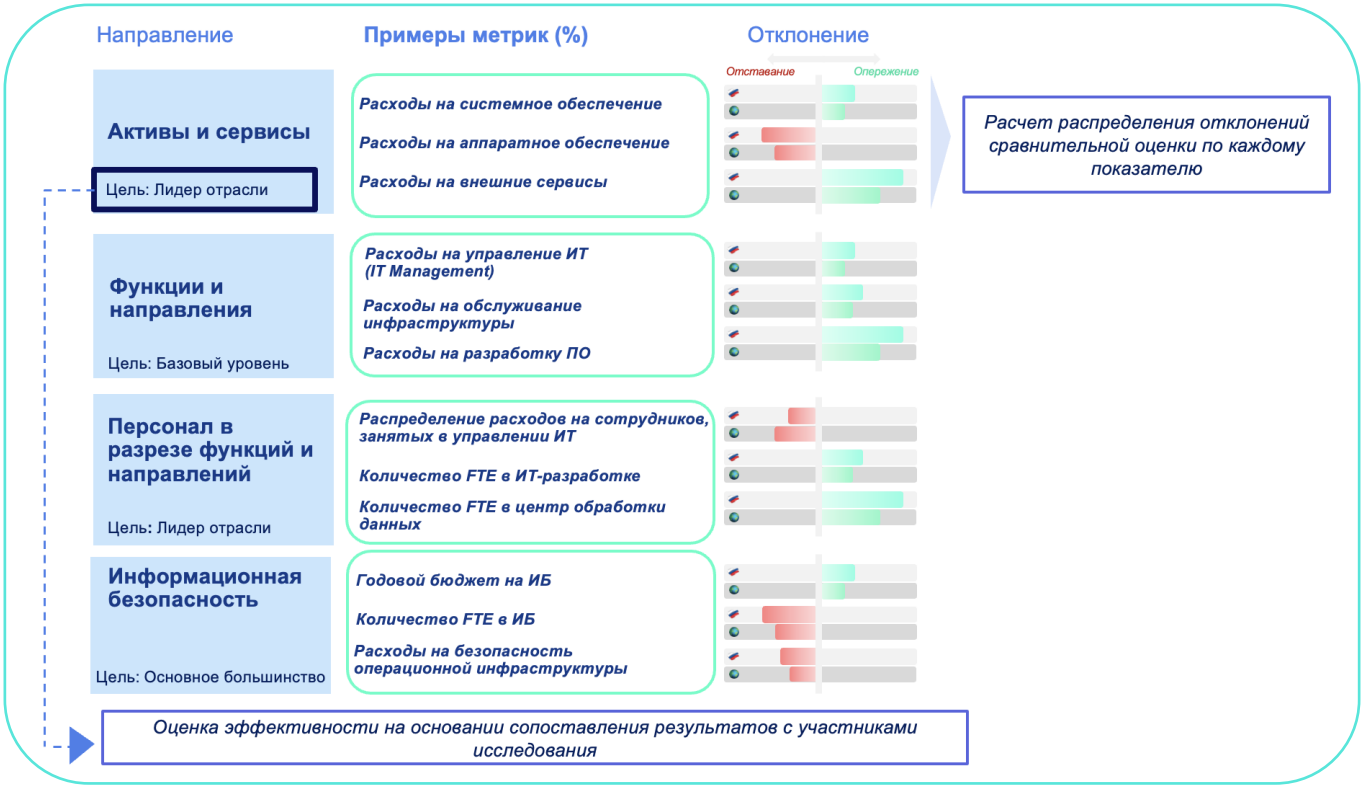
Исследование предполагает **сравнение показателей ИТ-подразделения** организации, **выявление отклонений** и **определение зон роста** с точки зрения эффективности расходов на ИТ по следующим аналитическим разрезам:

Технологический бенчмаркинг: 4 аналитических разреза

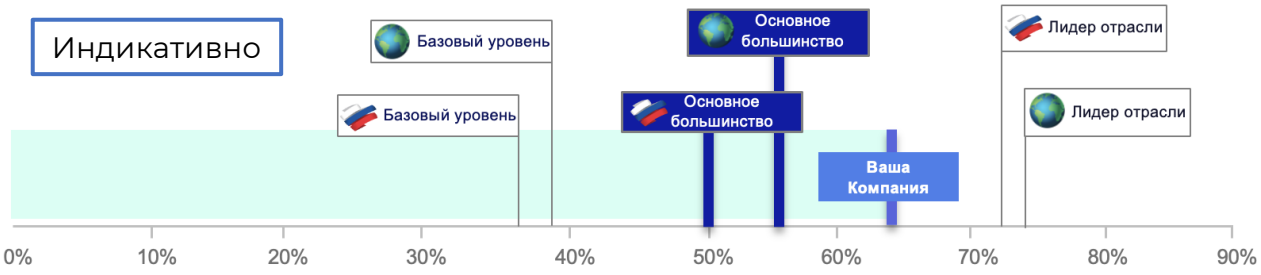
Примеры результатов отчета в рамках Технологического бенчмаркинга

Отчет представляет сопоставление с российскими и международными метриками в технологической отрасли, дает оценку эффективности использования распределения ИТ-затрат.

- **Пример дашбордов с бенчмарками**



- **Оценка уровня эффективности**



Результаты

Ваша Компания	62,5%
Цель: Основное большинство	50%
Цель достигнута с опережением на 12,5%	

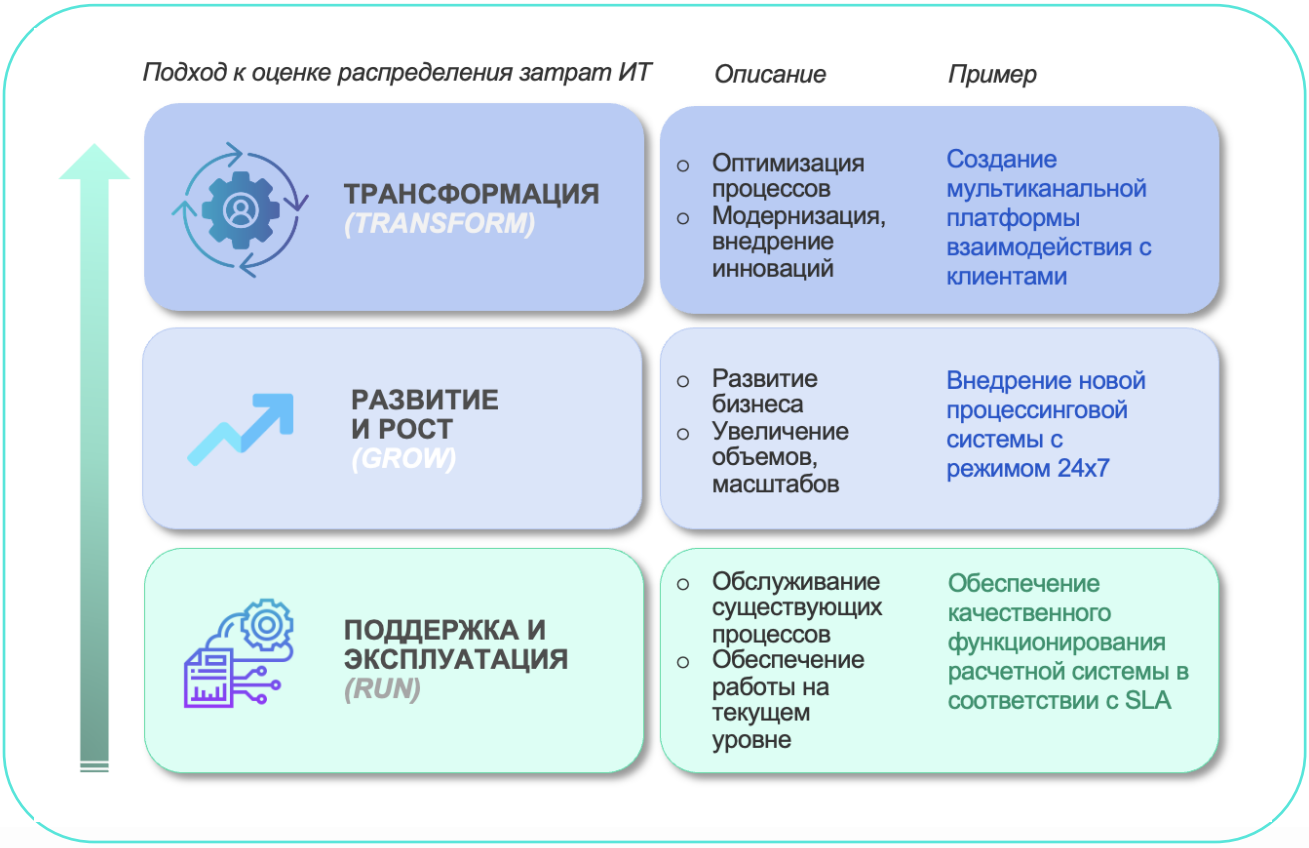
Отраслевой показатель

Базовый уровень	25й перцентиль	37,6%	39,3%
Основное большинство	50й перцентиль	50%	57,1%
Лидер отрасли	75й перцентиль	75%	75%

Бенчмаркинг, полученный на основе оценки по рынку России

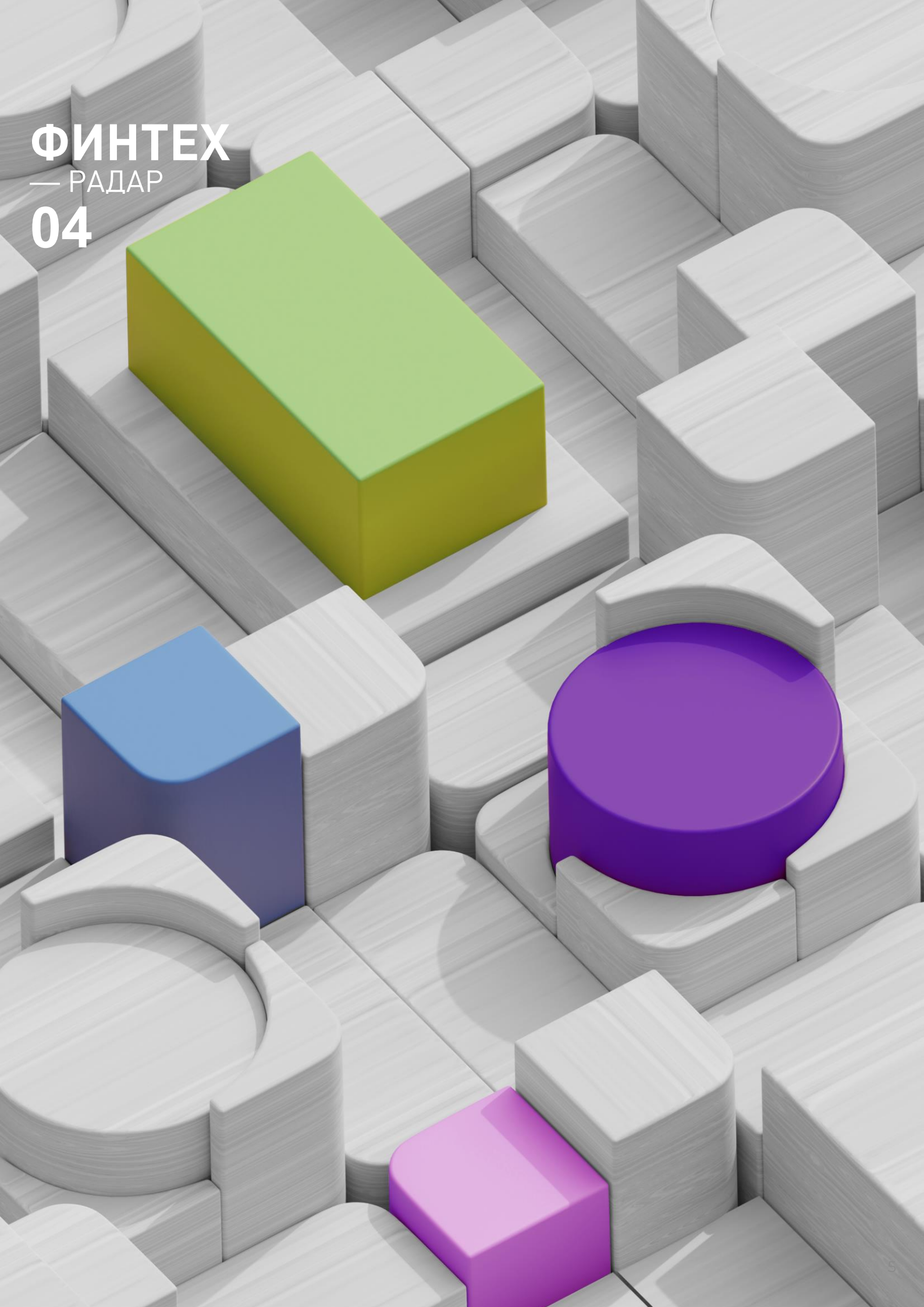
Бенчмаркинг, полученный исходя из мировых данных

В исследовании также будет представлен механизм для оценки распределения затрат ИТ по трем ключевым направлениям: **поддержка и эксплуатация (RUN), развитие и рост (GROW), трансформация (TRANSFORM).** Данная оценка позволит выявить возможные области усовершенствования управления ресурсами компании, их более эффективного перераспределения и запуска стратегических инициатив по цифровой трансформации бизнеса.



В условиях быстро развивающихся технологий и все большей зависимости бизнеса от информационных систем, обеспечение безопасности становится критически важным для любой компании. Одним из ключевых инструментов для обеспечения безопасности является использование **инструментария безопасной разработки**, который позволяет **выявлять и устранять уязвимости** на ранних стадиях создания ПО, а также **обеспечивает баланс между развитием и рисками.**

ФИНТЕХ
— РАДАР
04



Технология месяца

DevSecOps

Безопасная разработка и
решения с открытым исходным кодом

Еще 10–15 лет назад разработки решений с открытым исходным кодом (Open Source) в России практически не существовало. Согласно новостному агентству Cnews, Министр цифрового развития, связи и массовых коммуникаций РФ **Максут Шадаев** называет открытые решения «главным трендом и магистралью», подчеркнув их важность тезисом **«опенсорс – наше все»**. Перед страной стоит задача за короткий срок создать полноценные отечественные решения с открытой лицензией, которые смогут стать основой технологического развития страны.

«Опенсорс – наше все»*

Максут Шадаев
Министр цифрового развития,
связи и массовых коммуникаций РФ

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ С ОТКРЫТЫМ ИСХОДНЫМ КОДОМ: СТАНОВЛЕНИЕ ПОДХОДА И ОСНОВНЫЕ ПРИНЦИПЫ

До середины 1970-х годов компьютерный код рассматривался как элемент работы вычислительной техники. Организации разрабатывали собственные программы, и обмен кодом был распространенной практикой.

Однако в 1974 году было установлено, что программный код подлежит защите авторским правом. Издание проприетарного ПО стало отраслью, в которой быстро возникла жесткая конкуренция.

«Бунт» против устоявшихся практик начался в 1983 году, когда программист Ричард Столлман основал Фонд свободного программного обеспечения (Free Software Foundation) и разработал первую лицензию на ПО с *«авторским левом» (copyleft*[1]*)* – **GNU General Public License (GPL)**.

Термин «Open source» был сформирован лидерами мнений в 1998 году. Многие считали, что понятие «свободное ПО» слишком сильно подчеркивает «безвозмездность» программного обеспечения в качестве его основной ценности. Для продвижения новой системы идей была создана организация **Open Source Initiative (OSI)**, которая установила основные принципы индустрии и разместила соответствующие лицензии на открытое ПО.

Понятие **«открытое свободное программное обеспечение»** (ОСПО) относится к тем лицензионным договорам, которые соответствуют условиям и GNU GPL, и OSI, и в таком случае корректным будет использование выражения «FLOSS» – «Free/Libre and Open Source Software». В нынешнем правовом поле РФ проблемы «действительности» ОСПО-лицензий нет, так как все лицензии, соответствующие этим условиям, соответствуют и принятым в стране понятиям «открытая лицензия[2]» и **«свободное программное обеспечение»** (СПО)[3].

*Глава Минцифры Максут Шадаев на CNews FORUM Кейсы — о системно значимых ИТ-компаниях, суверенном интернете и «Гостехе»

[1] Авторское лево – лицензия, которая требует от каждого, кто улучшает исходный код, аналогичным образом публиковать его отредактированную версию свободно для всех.

[2] Статья 1286.1 ГК РФ. Открытая лицензия на использование произведения науки, литературы или искусства (введена Федеральным законом от 12.03.2014 N 35-ФЗ).

[3] ГОСТ Р 54593–2011. Национальный стандарт Российской Федерации. Информационные технологии. Свободное программное обеспечение. Общие положения (утв. и введен в действие Приказом Росстандарта от 06.12.2011 N 718-ст).

Для того, чтобы лицензионный договор можно было называть «открытым», он должен соответствовать **10 критериям**, опубликованным OSI[4]:

1 Свободное распространение

Лицензия не ограничивает никакую сторону в продаже или передаче программного обеспечения в качестве компонента совокупного распространения. Лицензия не требует выплаты роялти или иного вознаграждения за такую продажу.

2 Доступность исходного кода

Программа должна включать исходный код и допускать распространение как в виде исходного кода, так и в скомпилированном виде.

3 Возможность модифицировать и редактировать ПО

Лицензия должна разрешать модификации и производные работы и позволять распространять их на тех же условиях, что и лицензия исходного программного обеспечения.

4 Целостность авторского исходного кода

Лицензия может ограничивать распространение исходного кода в измененном виде только в том случае, если лицензия допускает распространение «файлов исправлений» вместе с исходным кодом с целью модификации программы во время сборки.

5 Отсутствие дискриминации лиц или групп лиц

Лицензия не должна дискриминировать какое-либо лицо или группу лиц.

6 Отсутствие дискриминации по целям применения

Лицензия не должна ограничивать использование программы в какой-либо конкретной области деятельности.

7 Распространение лицензии

Права, прилагаемые к программе, должны распространяться на всех, кому она перераспространяется, без необходимости оформления дополнительной лицензии.

8 Независимость от другого ПО

Права, предоставляемые программе, не должны зависеть от принадлежности программы к тому или иному дистрибутиву программного обеспечения

9 Отсутствие ограничений на иное ПО

Лицензия не должна накладывать ограничений на другие программы, распространяемые вместе с лицензионным программным обеспечением.

10 Технологическая нейтральность

Ни одно из положений лицензии не должно зависеть от какой-либо отдельной технологии или стиля интерфейса.

[4] Приводится короткая свободная интерпретация 10 принципов OSI. Для ознакомления с официальной трактовкой правительства РФ, указанной в постановлении к эксперименту по открытым лицензиям, рекомендуем ознакомиться с исходным текстом Постановления Правительства Российской Федерации от 10.10.2022 № 1804 на официальном интернет-портале правовой информации (www.pravo.gov.ru).

ОТЛИЧИЕ СВОБОДНОГО ПО И ОТКРЫТОГО ПО

Понятие **свободное ПО** (СПО), фигурирующее в законодательных проектах и нормативной базе Российской Федерации, **не эквивалентно** понятию **открытое ПО** (ОПО), используемого ИТ-специалистами.

Любое открытое ПО является свободным, однако не каждое свободное ПО является открытым

Сильно упрощая, свободное ПО – любое, которое не считается проприетарным[5].

Лицензии СПО можно разделить на «разрешительные» и «вирусные». Разрешительные лицензии не налагают серьезных ограничений, в том числе и по дальнейшей судьбе производных продуктов. В этот список можно включить такие лицензии, как Apache и MIT.

Их важно различать, так как приложение, использующее ПО с «вирусной» лицензией, будет сложно зарегистрировать в Едином реестре российских программ (ЕРРП). Необходимо будет убедиться[6], что этот компонент правомерно используется и позволяет получить исключительные права на ПО, использующее его в составе.

ПОРЯДОК ИСПОЛЬЗОВАНИЯ СВОБОДНОГО ПО

В рамках методических рекомендаций Минцифры по переходу на использование российского программного обеспечения[7] любое ПО, которое не зарегистрировано в одном из реестров приложений, **приравнивается к иностранному ПО.**

Таким образом, любое свободное ПО может использоваться субъектами критической информационной инфраструктуры финансового рынка (КИИ ФР)[8] только при выполнении следующих условий:

1. в Едином реестре российских приложений (ЕРРП) отсутствует полнофункциональный аналог необходимого решения;
2. в Реестре евразийского программного обеспечения (РЕПО) отсутствует отсутствует соответствующий полнофункциональный аналог.

Также имеется дополнительное условие – между двумя аналогичными приложениями, одно из которых зарегистрировано в дружественной стране, а другое в недружественной[9], **рекомендуется выбирать первое.**

Свободное ПО позволяет разработчикам создавать комбинации различных программных компонентов, что может способствовать появлению новых инновационных продуктов и сервисов. Например, если есть две программы с открытым кодом, одна из которых предназначена для создания веб-сайтов, а другая – для управления базами данных, то разработчик может объединить их функциональность, чтобы создать новый продукт, который сочетает в себе возможности обеих программ.

[5] Корректное определение можно найти в ГОСТ Р 54593-2011 «Информационные технологии. Свободное программное обеспечение. Общие положения».
[6] Подробнее об условиях включения программного обучения в ЕРРП: «Правила формирования и ведения реестров Российского и Евразийского программного обеспечения»
[7] Приказ Минцифры России от 18.01.2023 N 21 «Об утверждении Методических рекомендаций по переходу на использование российского программного обеспечения, в том числе на значимых объектах критической информационной инфраструктуры Российской Федерации, и о реализации мер, направленных на ускоренный переход органов государственной власти и организаций на использование российского программного обеспечения в Российской Федерации»
[8] Критической информационной инфраструктуры финансового рынка
[9] Распоряжение от 5 марта 2022 года №430-р «Перечень иностранных государств и территорий, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия».

ВОЗМОЖНОСТИ ОТКРЫТОГО ИСХОДНОГО КОДА (OPEN SOURCE)

Использование ПО с открытым кодом предоставляет значительные преимущества. Во-первых, **снижается время вывода продукта на рынок (T2M**). Поскольку разработчики могут использовать существующие решения и модифицировать их под свои нужды, время и затраты на разработку значительно сокращаются. Кроме того, открытый код обеспечивает более быстрый доступ к новым технологиям, что также способствует ускорению процесса разработки и выходу конечного продукта.

Во-вторых, с точки зрения DevSecOps, открытый код **обеспечивает большую прозрачность и контроль над безопасностью приложений**. Разработчики могут легко проверить код на наличие уязвимостей и исправить их до того, как они станут проблемой для пользователей.

Практика DevSecOps ускоряет вывод продукта на рынок, что приводит к росту выручки на 15-20%

Открытый код также позволяет применять **лучшие практики безопасности**, которые были созданы сообществом разработчиков – использование **проверенных библиотек** и **фреймворков**, а также реализация **глубоко проработанных** процессов разработки и тестирования безопасности.

Безопасная разработка снижает долю уязвимого корпоративного ПО в 2,5 раза

Открытый исходный код может помочь в соблюдении требований по безопасности и соответствию регуляторным нормативам. Компании могут использовать безопасные и проверенные решения, которые уже были протестированы сообществом разработчиков, а также иметь доступ к открытым стандартам и документации.

В рамках исследования **«Применение технологий искусственного интеллекта на финансовом рынке»,** разработанного **Ассоциацией ФинТех**, выявлено, что всего **15%** компонентов технологического стека опрошенных компаний составляют **иностранные проприетарные решения**. Более **75%** составляют либо **открытое ПО**, либо **собственные разработки** компаний, которые, в свою очередь, в значительной мере основываются на открытом исходном коде.

ДОЛЯ ТИПОВ ПО В ТЕХНОЛОГИЧЕСКОМ СТЕКЕ ИИ-СИСТЕМ КЛЮЧЕВЫХ ИГРОКОВ ФИНАНСОВОГО РЫНКА

ТОП-3 используемых решений по открытой лицензии

Управление данными

Управление жизненным циклом ML-модели

Управление данными

Популярность применения открытого исходного кода организациями российского финансового рынка также подтверждается результатами проведенного **исследования уровня технологической готовности и цифровой зрелости** – **все** опрошенные организации (100%) подтвердили, что **применяют открытое ПО** в своих разработках.

ВЫЗОВЫ ОТКРЫТОГО ИСХОДНОГО КОДА

Использование решений с открытым кодом становится все более распространенным, предоставляя множество преимуществ, таких как экономия времени и ресурсов на разработку. Однако такой подход, как и любой другой, также обладает рядом рисков.

ОГРАНИЧЕНИЯ ПО ЗАКУПКАМ ЛИЦЕНЗИЙ

Компания может столкнуться с ограничениями на использование открытого исходного кода в коммерческих целях или на продажу продуктов, основанных на этом коде. Некоторые лицензии могут также требовать, чтобы компания открыла свой собственный код и поделилась им с сообществом разработчиков. Это может привести к тому, что компания не сможет полностью контролировать свое ПО и не сможет получать прибыль от продажи продуктов, основанных на нем. Кроме того, ограничения по лицензированию могут привести к проблемам совместимости и функциональности, если организация не может использовать необходимые компоненты или библиотеки, которые требуются для работы ее ПО.

ОГРАНИЧЕНИЯ НА ЗАРУБЕЖНЫЕ ИТ-ПРОСТРАНСТВА

Компания может столкнуться с ограничениями на доступ к открытому исходному коду, хранящемуся за рубежом. Это может быть вызвано политическими, экономическими или юридическими причинами. Например, некоторые страны могут запретить доступ к отдельным сайтам или сервисам, которые содержат открытый код. Кроме того, некоторые страны могут требовать, чтобы организации хранили код своих решений на серверах внутри страны или использовали только локальные инструменты для разработки ПО. Это может привести к тому, что компания не сможет получить доступ к необходимым компонентам или библиотекам, которые хранятся в другой стране, что может привести к проблемам интероперабельности и функциональности ее ПО.

НАЛИЧИЕ ЗАКЛАДОК И BACKDOOR

Закладки – это специальные участки кода, которые могут быть внедрены в исходный код программного обеспечения, а также использованы злоумышленниками для получения доступа к корпоративным системам, нарушения конфиденциальности данных и проведения кибератак. Backdoor представляет собой скрытый канал в ПО, который может быть использован для получения несанкционированного доступа к системам и данным компании. Он может быть создан злоумышленниками или даже разработчиками с целью облегчения технической поддержки или обновления технического решения.

ОБНОВЛЕНИЕ ЗАВИСИМОСТЕЙ

В данном случае риск возникает из-за того, что многие программы используют сторонние библиотеки и компоненты, которые могут содержать уязвимости и лозунги. Обновление зависимостей может привести к нарушению работы приложения или даже к появлению новых уязвимостей. Например, если приложение использует для обработки изображений стороннюю библиотеку, содержащую уязвимость, то при ее обновлении ПО может перестать работать или стать уязвимой для кибератак.

НЕОБХОДИМОСТЬ В ОРГАНИЗАЦИИ ФОРКОВ

Риск возникает в случае, когда разработчикам необходимо изменить исходный код сторонней зависимости с целью исправить ошибку или добавить новый функционал. Если изначальная зависимость перестает поддерживаться сообществом, то разработчики могут быть вынуждены создавать собственную версию зависимости – форк. Форки создают дополнительные риски для проекта, так как могут привести к разделению кодовой базы и увеличению сложности поддержки. Кроме того, форки могут содержать свои уязвимости и ошибки, которые не будут исправлены в изначальной зависимости.

ОГРАНИЧЕНИЯ РОССИЙСКИХ АНАЛОГОВ ПО

Риск возникает в случае использования ПО, которое не соответствует законодательству РФ. Например, в России действует закон «О персональных данных», который устанавливает требования к обработке данных граждан России. Использование иностранного ПО, которое не соответствует этим требованиям, может привести к нарушению закона и штрафам. Кроме того, Россия также имеет свои национальные стандарты и требования к информационной безопасности, которые могут отличаться от международных. Из-за использования иностранного ПО, не соответствующего этим требованиям, могут повыситься риски для информационной безопасности.

Ключевой вызов открытого исходного кода – ограничение доступа к иностранному ПО

Таким образом, решения с открытым кодом имеют свои преимущества, такие как более прозрачный и доступный код, возможность участия в разработке и улучшении продукта, а также экономия на лицензионных платежах. Однако, при использовании таких решений необходимо учитывать и вышеупомянутые риски.

Для обеспечения безопасности ПО необходимо внедрять методы **безопасной разработки**. Это означает, что **безопасность должна обеспечиваться на всех этапах – от планирования до сопровождения конечного продукта**. Такой подход позволяет выявлять и устранять уязвимости на ранних этапах разработки, что снижает риски для пользователя.

БЕЗОПАСНАЯ РАЗРАБОТКА

В последние годы наблюдается резкий рост интереса к безопасной разработке ПО. Это обусловлено рядом факторов:

- увеличением числа кибератак и утечек данных;
- усилением нормативных требований к организациям по части информационной безопасности и защиты данных;
- зависимостью бизнеса от технологий.

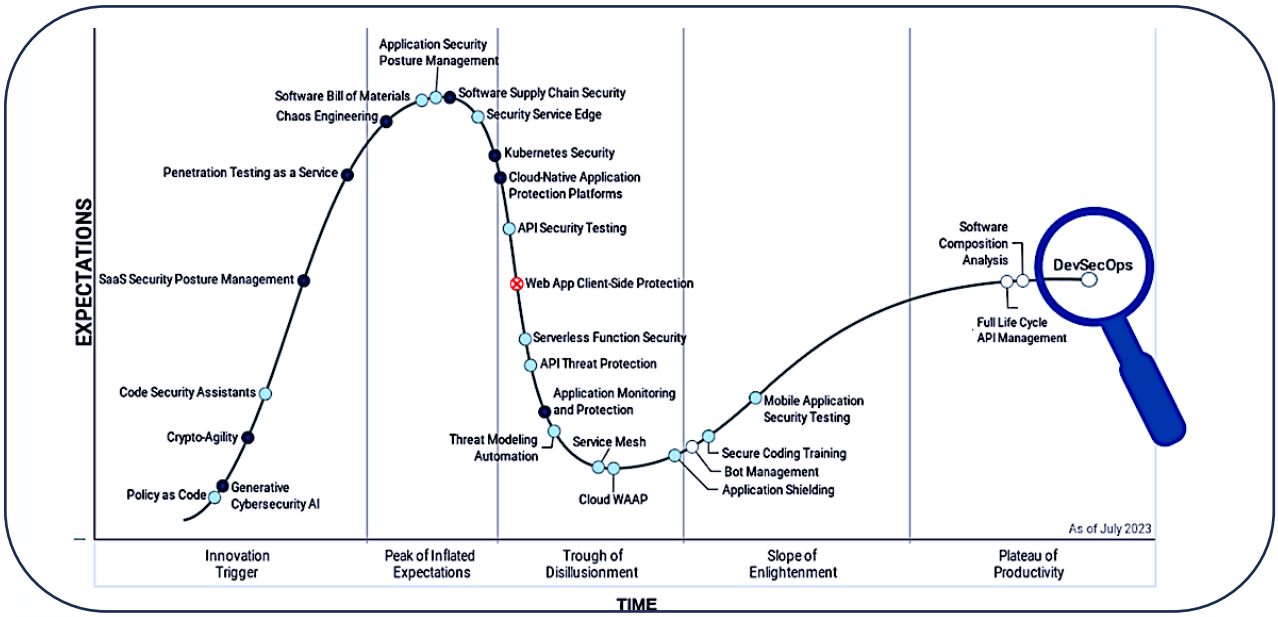
Безопасная разработка (DevSecOps) – подход к интеграции и автоматизации тестирования безопасности и соответствия нормативным требованиям в гибкие конвейеры разработки IT и DevOps, не снижающий гибкость и скорость работы разработчиков и не требующие от них выхода из системы разработки.

Безопасная разработка может быть внедрена как в последовательных моделях организации процесса (Waterfall), так и в гибких методологиях (Agile, DevOps). В данном материале фокус сделан на гибких подходах, так как именно они наиболее часто используются в проектах технологических лидеров.

ВАЖНОСТЬ БЕЗОПАСНОЙ РАЗРАБОТКИ

DevSecOps – это средство эффективной интеграции практик информационной безопасности в процесс разработки, позволяющее устранить или уменьшить трения между безопасностью и разработкой. Целью DevSecOps является достижение безопасного и работоспособного жизненного цикла разработки ПО (Software Development Life Cycle, SDLC). Безопасная разработка является развитым технологическим подходом по мнению аналитического агентства Gartner. В недавно опубликованном отчете[10] об актуальных трендах и этапах развития технологий в обеспечении безопасности предложений, эксперты оценили уровень развития DevSecOps как «зрелый мейнстрим».

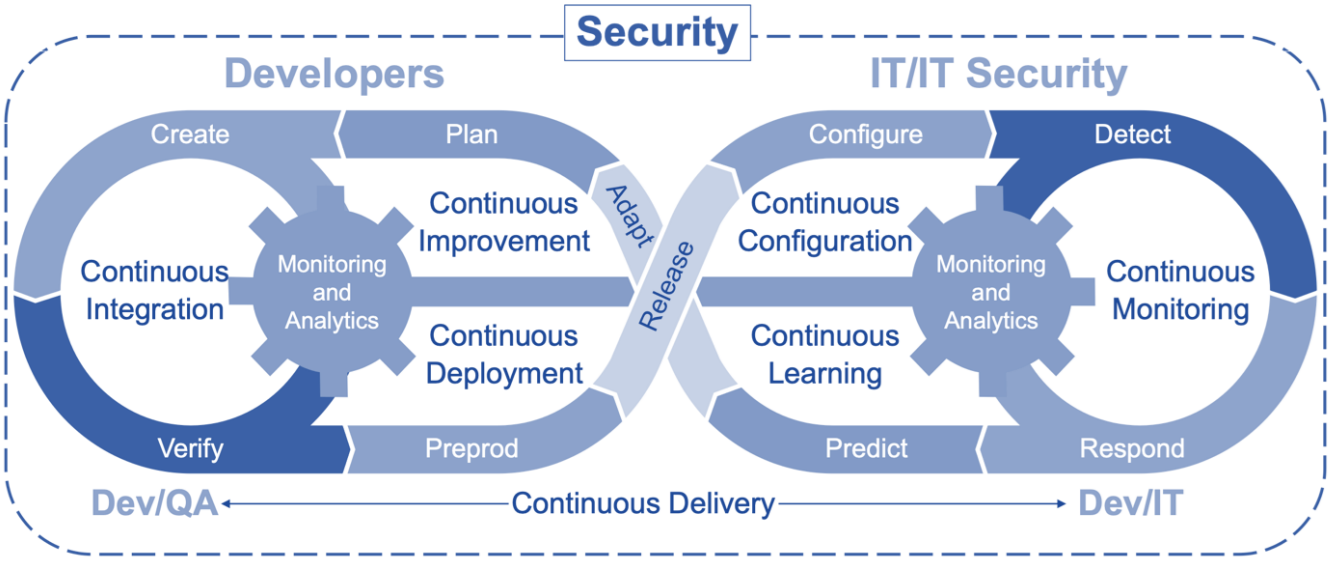
GARTNER HYPE CYCLE FOR APPLICATION SECURITY, 2023



[10] Gartner: Hype Cycle for Application Security, 2023

Стимулом для укрепления позиций концепции безопасной разработки является значительное повышение риска непреднамеренного использования разработчиками известных уязвимых компонентов и фреймворков при использовании открытого исходного кода. Подход DevSecOps стоит применять как можно раньше в процессе разработки, в то время как традиционные средства тестирования безопасности приложений (AST), связанные с более старыми моделями разработки, применяются на поздних этапах цикла и вызывают недовольство разработчиков и корпоративных стейкхолдеров.

ЦИКЛ БЕЗОПАСНОЙ РАЗРАБОТКИ GARTNER



ОСНОВНЫЕ ПРАКТИКИ DEVSECOPS

Подавляющая доля нарушений безопасности происходит по причине использования злоумышленниками известных программных ошибок. Поэтому крайне важно устранять уязвимости на этапе разработки ПО для снижения рисков информационной безопасности. Существует ряд технологий, которые помогают выявлять недостатки безопасности на ранних этапах и устранять их до релиза продукта:

Системы анализа состава ПО (SCA) – специализированные средства обеспечения безопасности приложений, позволяющие обнаруживать открытое ПО и компоненты сторонних производителей, имеющие уязвимости в системе безопасности, выявлять потенциально неблагоприятные риски лицензирования и цепочки поставок. SCA сегодня считается основополагающим элементом тестирования безопасности приложений (AST).

Тестирование безопасности приложений (AST) – процесс выявления и устранения уязвимостей в приложениях. Он может выполняться вручную или быть автоматизирован.

Кроме SCA существуют и другие типы AST, в том числе:

Статическое тестирование (SAST) – в рамках подхода происходит сканирование исходного кода приложения на наличие потенциальных уязвимостей;

Динамическое тестирование (DAST) – в рамках подхода производится симулирование атак на приложение для проверки уязвимостей;

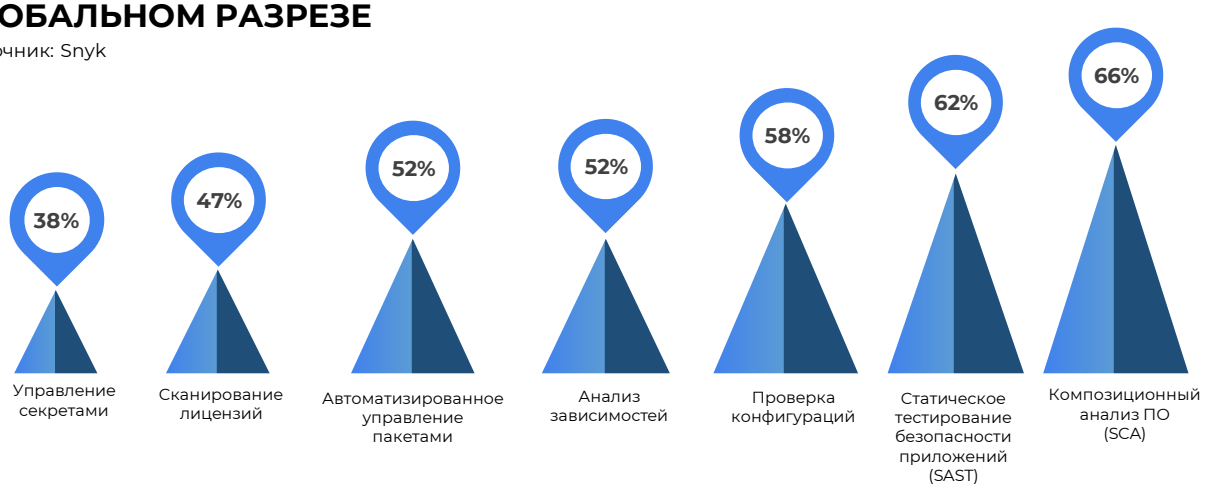
Интерактивное тестирование (IAST) – подход сочетает в себе практики SAST и DAST, динамически анализируя приложение во время его работы.

[10] Gartner: Hype Cycle for Application Security, 2023

Глобально в рамках безопасной разработки компании **наиболее активно применяют композиционный анализ ПО (66%) и статическое тестирование безопасности приложений (SAST) (62%).** Также значительную популярность имеют проверка конфигураций (58%), автоматизированное управление пакетами и анализ зависимостей (52%). Эти инструменты позволяют обеспечить высокий уровень безопасности при разработке программного обеспечения, что является критически важным в современном мире информационных технологий.

ВНЕДРЕННЫЕ ПРОЦЕССЫ DEVSECOPS В ГЛОБАЛЬНОМ РАЗРЕЗЕ

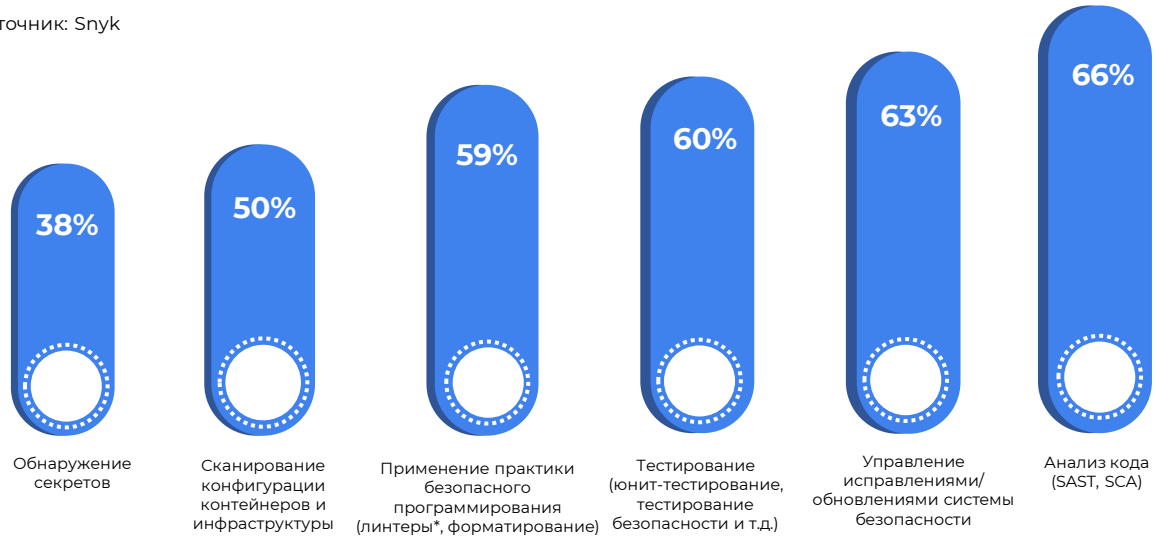
Источник: Snyk



Несмотря на то, что количество кибератак с каждым годом увеличивается, в частности, на открытый код, **40% мировых организаций по-прежнему не используют две наиболее фундаментальные технологии цепочки безопасности – SCA и SAST**. Еще меньшее число компаний применяют «облачные» меры безопасности, такие как проверка конфигурации инфраструктуры как инструмента кода и сканирование секретов[11].

АВТОМАТИЗИРОВАННЫЕ ПРОЦЕССЫ DEVSECOPS

Источник: Snyk



Автоматизация мер безопасности на различных этапах жизненного цикла разработки осуществляется **в большей степени** при **анализе кода** (66%), **управлении исправлениями системы безопасности** (63%), в **процессах тестирования** (60%), а также в применении **практики безопасного программирования** (59%).

Устранение последствий инцидента выходит гораздо дороже, чем применение мер по недопущению изъянов. Практики безопасной разработки позволяют создать продукты, которые содержат меньшее число уязвимостей. Так организации сокращают затраты на доработки продуктов после проведения финальных тестов безопасности.

[11] Управление секретами – это практика, позволяющая разработчикам надежно хранить конфиденциальные данные, такие как пароли, ключи и маркеры, в защищенной среде со строгим контролем доступа.

* Линтер – программа, проверяющая код на соответствие стандартам, согласно определенному набору правил. Правила описывают отступы, названия создаваемых сущностей, скобки, математические операции и другие аспекты.

РЫНОЧНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОЙ РАЗРАБОТКЕ

Развитие новых инструментов и технологий способствует увеличению интереса к безопасной разработке, и на российском рынке представлены эффективные продукты для статического, динамического и интерактивного анализа кода, решения по обнаружению уязвимостей в автоматическом режиме, мониторинг сетевой активности и пр. С точки зрения конкурентоспособного технологического стека **Россия занимает сильную позицию** – на отечественном рынке **присутствуют ключевые системные инструменты сборки, анализа и тестирования**, обеспечивающие **полный цикл безопасной разработки**.

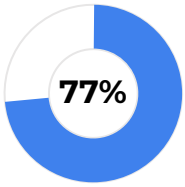
На сегодняшний день под угрозой кибератак находятся не только крупные финансовые организации, но практически любая российская компания с ИТ-инфраструктурой. Так, РТК-Солар, провайдер сервисов и технологий ИБ, отметила, что **количество инцидентов[12] в рамках информационной безопасности** во 2 квартале 2023 г. **выросло на 12%** в сравнении с 1 кварталом 2023 г., а также более, чем на **75%** в сравнении с 1 кварталом 2022 г. В другом отчете[13] РТК-Солар отмечает, что киберпреступники сменили ландшафт угроз. Это связано с тем, что значительно повысились объем идеологически мотивированных атак и количество автоматизированных инструментов, облегчающих типовые кибератаки.

Хакеры чаще стали прибегать к кибермразведке, а атаки становятся все более сложными. На сегодняшний момент невозможно полностью защититься, создавая только периметр безопасности. **Огромное количество уязвимостей возникает непосредственно в коде приложений, и устранять их достаточно затруднительно, особенно когда приложение уже разработано.** На рынке встал вопрос безопасности используемого открытого кода, так как с недавних пор в него стали добавляться закладки[14] и иной контент, нежелательный для российских организаций.

«Практики безопасной разработки помогают обеспечить надлежащую безопасность итогового продукта компании и ускорить процесс его вывода на рынок. Именно поэтому DevSecOps оказался актуален, как никогда».

Сергей Демидов
Директор Департамента операционных рисков,
информационной безопасности и непрерывности бизнеса
Московской Биржи

Согласно оценкам заместителя генерального директора, «Гарда Технологии» Владимира Пономарева, при внедрении практик безопасной разработки можно **«смело прибавлять 7–10% к текущим затратам на разработку».** Кроме того, при использовании инструментов на базе ИИ, генерирующих код, отмечается повышение уровня безопасности разработки.



компаний отметили повышение качества безопасной разработки при использовании инструментов ИИ, генерирующих код

По мнению Gartner, внедрение DevSecOps-практик позволяет сократить общие затраты на проект на 25%.

[12] РТК-Солар: «Атаки на российские компании во II квартале 2023 года».
[13] РТК-Солар: «Отчет о ключевых внешних цифровых угрозах для российских компаний».
[14] Закладкой (или программной закладкой) в информационной безопасности называют скрытно внедренную в защищенную систему программу, либо намеренно измененный фрагмент программы, которая позволяет злоумышленнику осуществить несанкционированный доступ к ресурсам системы на основе изменения свойств системы защиты.

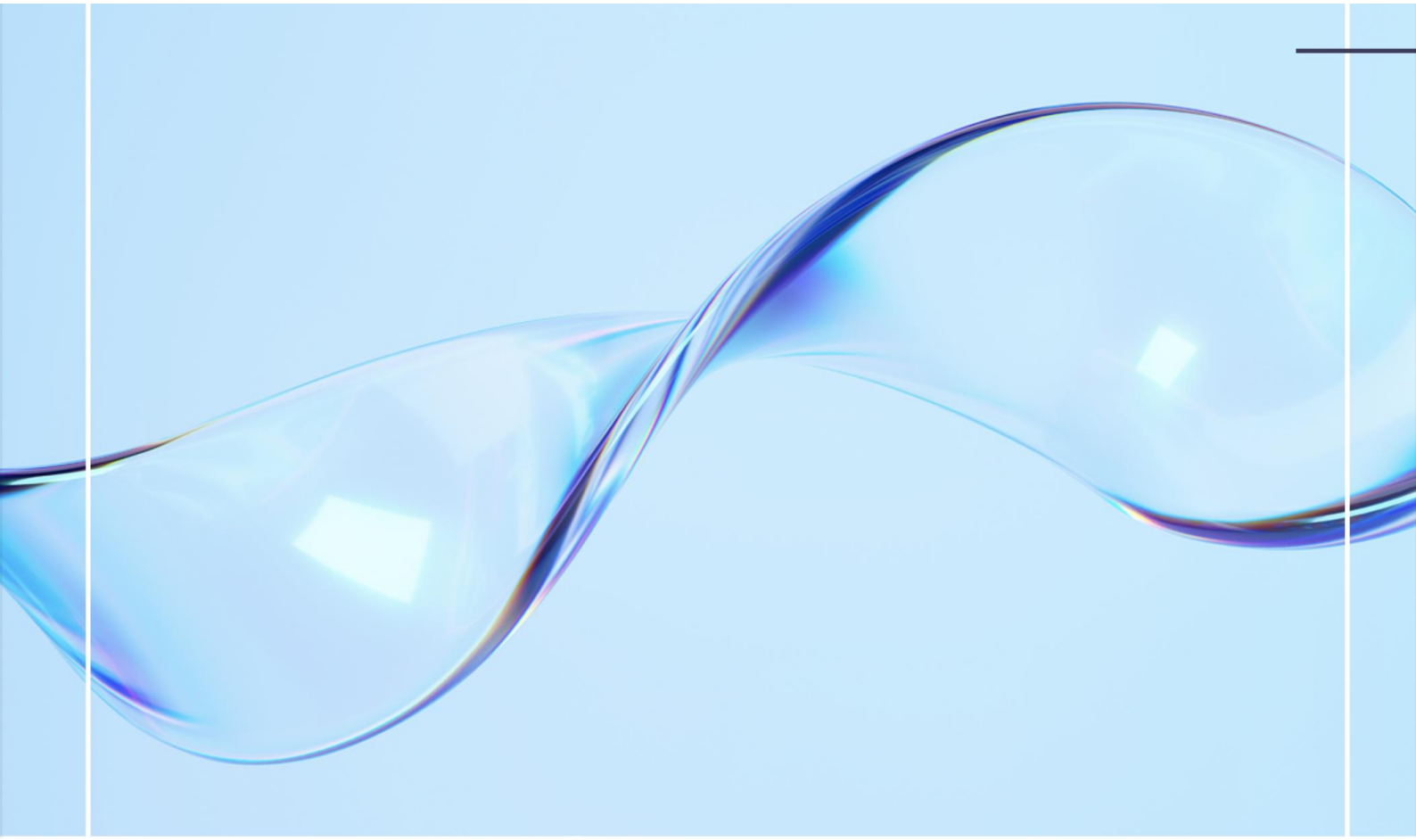
РЕГУЛЯТОРНЫЕ ТРЕБОВАНИЯ К БЕЗОПАСНОЙ РАЗРАБОТКЕ

Требования к безопасности ПО в финансовом секторе прописаны в положениях Банка России 683-П[15] и 757-П[16]. Они обязывают финансовые организации использовать ПО, которое либо прошло оценку в системе сертификации Федеральной службы по техническому и экспортному контролю (ФСТЭК), либо прошли оценку соответствия по требованиям к оценочному уровню доверия (далее – ОУД) не ниже, чем ОУД 4, в соответствии с требованиями национального стандарта ГОСТ 15408[17].

Система сертификации ФСТЭК сильно перегружена. Срок проверки одного экземпляра ПО составляет полгода, а иногда достигает 9–12 месяцев. При надлежащей частоте релизов банковского ПО в 2 недели данное условие выглядит мало приемлемым.

По этой причине финансовые организации присматриваются к ГОСТ Р 15408. Механика работы ГОСТ Р 15408 неочевидная: стандарт описывает только общие практики к обеспечению безопасности ПО. Поэтому Банк России разработал методический документ «Профиль защиты»[18] для финансового сектора, покрывающий как требования к безопасности ПО общего назначения, так и требования со стороны Банка России для кредитных и некредитных финансовых организаций.

Безопасная разработка – эффективный инструмент снижения общего страхового киберриска.



[15] Положение Банка России от 17.04.2019 N 683-П (ред. от 18.02.2022) «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента».

[16] Положение Банка России от 20.04.2021 N 757-П (ред. от 20.04.2021) «Об установлении обязательных для некредитных финансовых организаций требований к обеспечению защиты информации при осуществлении деятельности в сфере финансовых рынков в целях противодействия осуществлению незаконных финансовых операций».

[17] ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности».

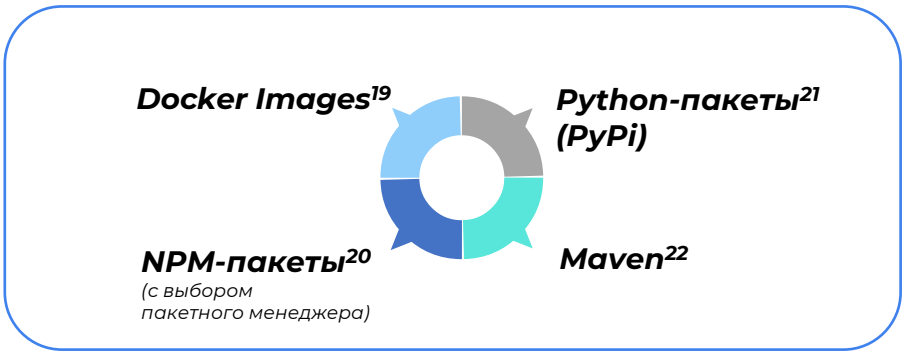
[18] Полное наименование: «Профиль защиты прикладного программного обеспечения автоматизированных систем и приложений кредитных организаций и некредитных финансовых организаций».

БЕЗОПАСНАЯ РАЗРАБОТКА: КЕЙС МОСКОВСКОЙ БИРЖИ

В качестве примера практического кейса применения безопасной разработки рассмотрим опыт члена Ассоциации ФинТех – **Московской Биржи**:

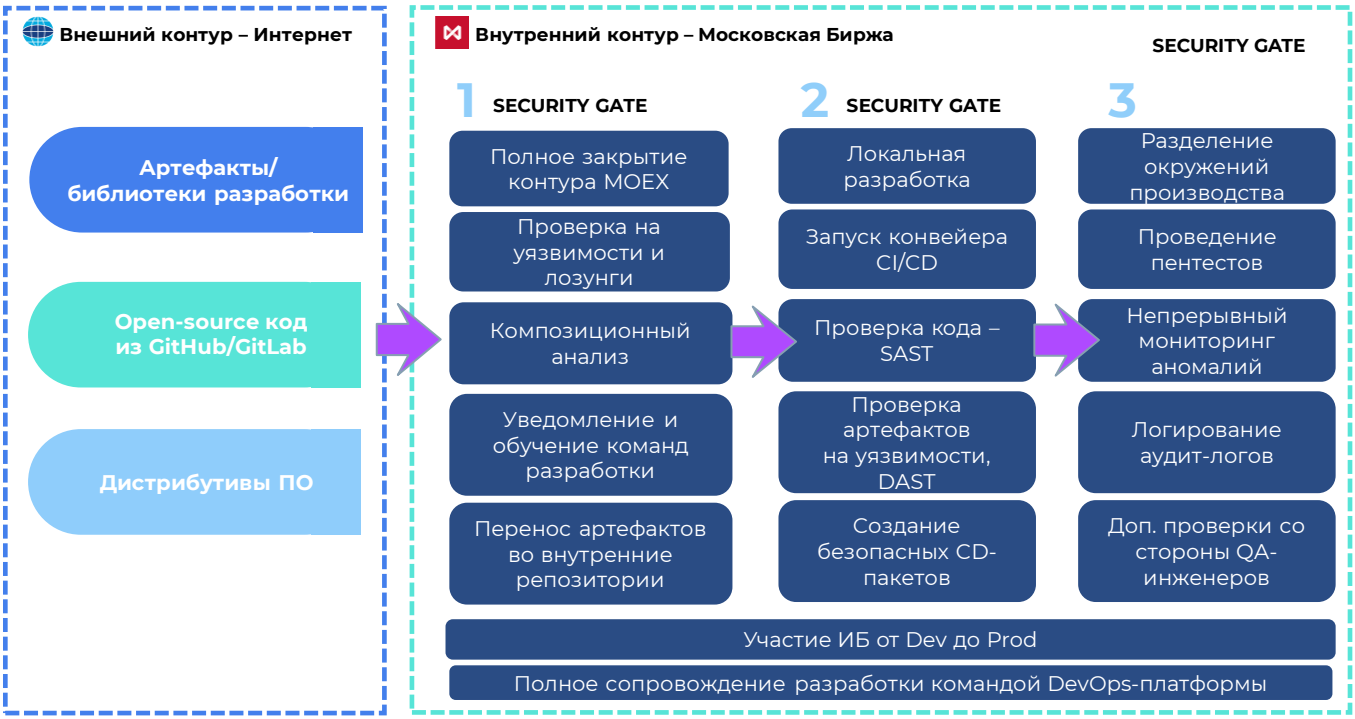
ФУНКЦИОНАЛ БЕЗОПАСНОГО ИСПОЛЬЗОВАНИЯ ВНЕШНИХ БИБЛИОТЕК

В рамках безопасной разработки на платформе DevOps существует сервис **DOPSecurity**. Данный продукт используется для автоматической загрузки объектов проверки и зависимостей в карантин с последующей передачей на проверку специалистам Лаборатории информационной безопасности. После прохождения проверки, на платформе доступен отчет и резолюция по допустимости использования объектов. На настоящий момент доступны следующие типы загрузок:



Особенность решения в том, что сервис не только загружает объекты и зависимости в карантин, но еще и проводит сканирование данных артефактов[23] автоматизированными средствами, что сокращает трудоемкость и время проверки. Это стало особенно актуально, когда многие внешние артефакты стали содержать в себе закладки и лозунги.

ФУНКЦИОНАЛ SECURITY GATES В КОНВЕЙЕРАХ РАЗРАБОТКИ И В ПРАКТИКЕ НЕПРЕРЫВНОЙ ИНТЕГРАЦИИ И ДОСТАВКИ (CI/CD)



В каждом из конвейеров внедрены этапы проверки кода и артефактов на уязвимости по базам данных уязвимостей.

[19] Docker Images – шаблоны (образы) для создания контейнеров в Docker, содержащие все необходимые компоненты, такие как операционная система, приложения, библиотеки и другие зависимости

[20] Node Package Manager (NPM) – менеджер пакетов для языка программирования JavaScript. Он позволяет устанавливать и управлять зависимостями проекта, а также использовать готовые модули и библиотеки, созданные другими разработчиками. NPM входит в состав Node.js – среды выполнения JavaScript на сервере

[21] Python-пакеты – наборы модулей, которые позволяют расширять функциональность языка Python. Могут содержать как стандартные библиотеки, так и сторонние модули, разработанные сообществом Python.

[22] Maven – инструмент для управления проектами на языке программирования Java.

[23] Артефакт — это любой созданный искусственно элемент программной системы. К элементам программной системы, а, следовательно, и к артефактам, могут относиться исполняемые файлы, исходный код, веб страницы, справочные файлы и многое другое, являющееся носителем информации.

ЦЕНТР КОМПЕТЕНЦИЙ ПО БЕЗОПАСНОЙ РАЗРАБОТКЕ АФТ

Ассоциация ФинТех совместно с **Московской Биржей** и другими ключевыми участниками финансового рынка создают отраслевой центр компетенций по безопасной разработке и проверке решений на основе свободного программного обеспечения (СПО).

Цель создания центра: обеспечение понятного и прозрачного процесса внедрения безопасной разработки и использования свободного программного обеспечения на финансовом рынке.

ОСНОВНЫЕ ЗАДАЧИ ЦЕНТРА:

- **Консолидация опыта, знаний и компетенций** участников АФТ по безопасной разработке и применению СПО;
- **Анализ и разъяснение требований**, **формирование предложений и рекомендаций** по совершенствованию нормативного регулирования;
- Согласование **типового технологического стека**;
- **Разработка и поддержка методологии** процессов безопасной разработки;
- Организация **обучения** специалистов;
- **Поддержка и консультация** специалистов и участников АФТ;
- **Идентификация, оценка и тестирование** ИТ-решений на основе СПО;
- **Организация совместных проектов** по развитию ИТ-решений на основе СПО.

*«Вместе с специалистами Московской Биржи планируем создать **сообщество экспертов**, совместная работа которых **упростит процесс внедрения DevSecOps**, что приведет к **повышению уровня защищенности разрабатываемых решений** и, как результат, выполнению задачи достижения требуемого уровня технологической независимости организаций»*

Олег Моргун
Руководитель Управления развития технологий АФТ

Для решения задач по размещению, хранению и проверке решений на основе открытого кода будет использоваться созданный АФТ **Репозиторий ИТ-решений для финансовой отрасли**. Реализация проектов по развитию ИТ-решений на основе СПО будет происходить на платформе ранее запущенной **Технологической песочницы АФТ**.

РЕКОМЕНДАЦИИ

Безопасность приложений является одним из **важнейших аспектов** при разработке программного обеспечения. Необходимо учитывать потенциальные уязвимости и риски, связанные с конфиденциальной информацией, а также возможностью атак со стороны злоумышленников. Таким образом, при внедрении безопасной разработки необходимо **руководствоваться комплексом мер**:

1 ОЦЕНИВАТЬ РИСКИ

Применение инструментария безопасной разработки для каждой строчки кода на практике не реализуемо. Организация должна понимать, **насколько безопасной** должна быть разработка, и сосредоточить усилия на ПО, подверженном наибольшему риску.

2 ПЛАНИРОВАТЬ ПРОЦЕСС ВНЕДРЕНИЯ БЕЗОПАСНОЙ РАЗРАБОТКИ

Необходимо **спланировать внедрение** безопасной разработки и **выработать метрики** для каждого этапа. Так получится оценивать успешность внедрения, и метриками смогут быть результаты проверки безопасности итогового продукта. Эти же метрики помогут оценить **экономический эффект внедрения** безопасной разработки, поскольку будет видно, как каждый этап влияет на общий уровень безопасности конечного продукта. Может выясниться, что часть инструментария безопасной разработки в действительности не нужна, поскольку не добавляет ожидаемого уровня безопасности.

3 ВЫБИРАТЬ ИНСТРУМЕНТЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

Выбор инструментария для безопасной разработки обширен, даже после ухода зарубежных вендоров. Замглавы Минцифры Александр Шойтов заявил, что **доля российских средств защиты информации** на рынке составляет около **90%**. Многие инструменты распространяются по открытой лицензии. С них и стоит **начинать внедрение практик безопасной разработки**, поскольку они позволяют запустить процесс без серьезных инвестиций. Определив узкие места, инструментарий в них можно будет усилить, а где-то обойтись базовыми решениями.

4 УКРЕПЛЯТЬ ВЗАИМОДЕЙСТВИЕ МЕЖДУ РАЗВИТИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Между разработчиками и специалистами по информационной безопасности должен быть выстроен **здравый диалог**. У продуктовой команды должны быть выставлены сбалансированные КПЭ как по метрикам безопасности, так и по времени сдачи проекта.

ПЕРСПЕКТИВЫ БЕЗОПАСНОЙ РАЗРАБОТКИ

Рынок кибербезопасности Российской Федерации **по результатам 2022 года** оценивается[24] в **193,3 млрд руб**., а **к 2027** должен составить **559 млрд руб**. На рынке продуктов средств защиты информации (СЗВ) в 2022 году **положение российских вендоров усилилось**: они занимают **70%** рынка. Прирост доли рынка от года в год составил 15%.

На настоящий момент Правительством РФ проводится **эксперимент по созданию условий для использования программного обеспечения в условиях открытой лицензии[25]**. Основными целями эксперимента заявляются обеспечение повторного использования программ для ЭВМ и внедрение передовых практик создания и развития ПО. В рамках данного эксперимента **планируется ввести русскоязычные открытые государственные лицензии**, которые будут **одновременно соответствовать и требованиям OSI к открытым лицензиям, и гражданскому кодексу РФ**, а также не предусматривать авторское лево (copyleft).

В то же время проводится **эксперимент по созданию национального репозитория** – отечественного аналога GitHub. Основными целями эксперимента в РФРИТ определили:

- **поддержку сообщества разработчиков** ПО с открытым кодом;
- создание **среды** для их совместной работы;
- увеличение участия **российских компаний** в разработке.

Безопасный доверенный репозиторий, соответствующий требованиям Минцифры, будет **создаваться и на базе Ассоциации ФинТех.**

Решения с открытым кодом являются важным фактором для развития финансового сектора, так как они представляют собой наиболее современные технологические практики, позволяют гибко их настраивать под нужды конкретного продукта и обходятся дешевле, чем проприетарные аналоги. Благодаря доступности кода разработчики могут анализировать его на предмет уязвимостей и исправлять их, что способствует повышению уровня безопасности приложений. Разработчики и организации финансового сектора должны уделять особое внимание использованию открытого кода и обеспечению его безопасности для защиты пользователей и повышения доверия к сервисам.

Таким образом, **безопасная разработка – это не только обеспечение безопасности, но и безопасного развития.** Практики безопасной разработки позволяют обеспечить баланс между рисками и развитием, необходимый российскому финтеху.

*Особая благодарность **Сергею Демидову** за помощь в подготовке материала*

[24] Центр стратегических инициатив: «Прогноз развития рынка кибербезопасности в Российской Федерации на 2023-2027 годы».

[25] Подробнее в постановлении Правительства Российской Федерации от 10.10.2022 № 1804 «О проведении эксперимента по предоставлению права использования программ для электронных вычислительных машин, алгоритмов, баз данных и документации к ним, в том числе исключительное право на которые принадлежит Российской Федерации, на условиях открытой лицензии и созданию условий для использования открытого программного обеспечения».

ПОЧИТАТЬ ДОПОЛНИТЕЛЬНО ПО ТЕМЕ

РТК-Солар

Отчет о ключевых внешних цифровых угрозах для российских компаний в январе-апреле 2023 года

Endor Labs

Топ-10 рисков, связанных с открытым исходным кодом

АНО «Открытый код»

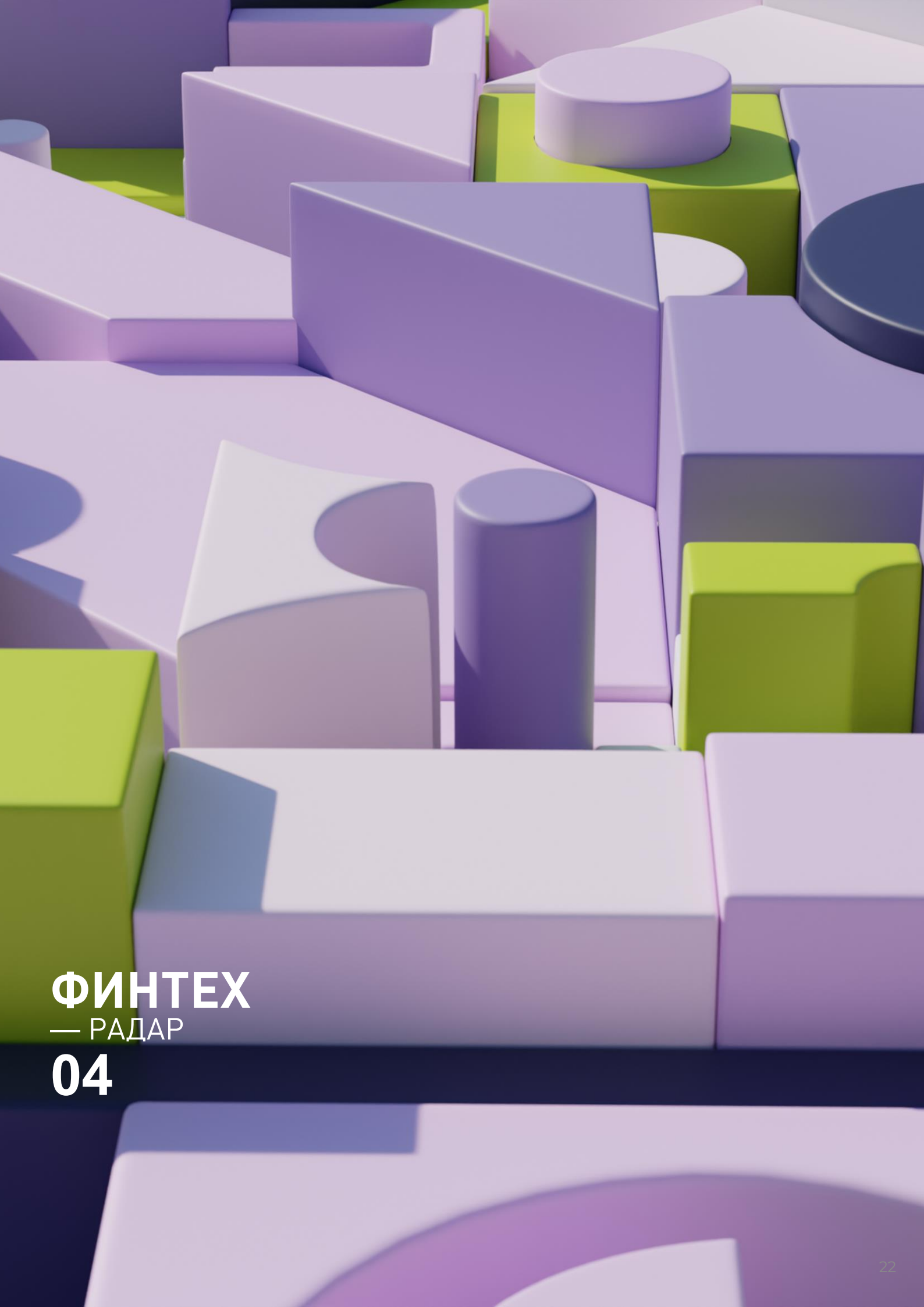
О корректном использовании ОСПО–компонент при создании и коммерциализации программных продуктов

Open Logic x OSI

Отчет о состоянии открытого ПО на 2023 год

Red Hat

Отчет о состоянии открытого ПО на предприятиях: финансовый сектор



ФИНТЕХ
— РАДАР
04

Техно-события

MCKINSEY СОСТАВИЛ РУКОВОДСТВО ПО ГЕНЕРАТИВНОМУ ИИ ДЛЯ CIO

В данном материале эксперты предлагают руководителям ИТ-подразделений сфокусироваться на **9 ключевых действиях** при внедрении генеративного ИИ:

1. Определить позицию компании в отношении внедрения генеративного ИИ и ознакомить с ней сотрудников.
2. Определить примеры использования генеративного ИИ, которые повышают ценность бизнеса.
3. Попытаться сосредоточиться на развитии потенциала генеративного ИИ при разработке ПО, сокращении технического долга и минимизации ручного труда.
4. Воспользоваться существующими сервисами или адаптировать модели с открытым исходным кодом для разработки собственных решений.
5. Модернизировать технологическую архитектуру предприятия для эффективной интеграции и управления моделями генеративного ИИ.
6. Разработать инфраструктуру данных, обеспечивающую качественный доступ к данным из различных источников.
7. Создать централизованную команду по разработке платформы генеративного ИИ, которая будет обеспечивать продуктовые и прикладные команды утвержденными моделями.
8. Вкладывать средства в повышение квалификации ключевых специалистов, таких как разработчики ПО, инженеры по данным, инженеры MLOps и специалисты по безопасности.
9. Оценить и смягчить риски, связанные с моделями, данными и законодательством в новом ландшафте генеративного ИИ.

IBM ОПУБЛИКОВАЛ ОТЧЕТ «ГЕНЕРАТИВНЫЙ ИИ В ОРГАНИЗАЦИЯХ: СОВРЕМЕННОЕ СОСТОЯНИЕ РЫНКА»

Средний ROI проектов с использованием генеративного ИИ растет, и руководители компаний ожидают, что к 2025 году он превысит 10%. В связи с этим организации планируют повысить темпы внедрения технологии в ближайшие два года. Если в 2022 году только 23% руководителей заявили, что в их организациях был опробован, внедрен, эксплуатируется или оптимизирован генеративный ИИ, то к 2024 году этот показатель вырастет до 62%. Руководители считают, что внедрение генеративного ИИ открывает такие возможности, как повышение качества контента, стимулирование конкурентоспособности и расширение компетенций сотрудников. В целом они в большей степени нацелены на расширение потенциала и обеспечение роста за счет повышения качества о

ЕВРОКОМИССИЯ ПРЕДСТАВИЛА СТРАТЕГИЮ ПО РАЗВИТИЮ МЕТАВСЕЛЕННОЙ

Стратегия, представленная Еврокомиссией, разработана в контексте цифровизации и ее влияния на экономику ЕС после 2030 года. В докладе говорится, что объем мирового рынка виртуальных миров вырастет с €27 млрд в 2022 году до более чем €800 млрд к 2030 году.

В отчете сформулированы четыре «ключевых столпа стратегии»:

1. **Люди:** расширение возможностей и укрепление навыков для повышения осведомленности, доступа к достоверной информации и формирования кадрового резерва специалистов по виртуальным мирам.
2. **Бизнес:** поддержка европейской индустриальной экосистемы Web 4.0 для наращивания передового опыта и устранения фрагментации.
3. **Правительство:** поддержка общественного прогресса и виртуальных госуслуг внутри виртуальных миров. Комиссия запускает два новых государственных проекта:
   - ***CitiVerse*** – иммерсивная городская среда, которая может быть использована для целей планирования и управления городом;
   - Европейский ***цифровой двойник человека***, который будет дублировать человеческое тело для поддержки принятия клинических решений и индивидуального лечения.
4. **Инфраструктура:** формирование стандартов для открытых и взаимодействующих виртуальных миров и Web 4.0, исключающих доминирование в них нескольких крупных игроков.

GITHUB И РЯД ДРУГИХ КОМПАНИЙ ПРИЗЫВАЮТ К РАСШИРЕНИЮ ПОДДЕРЖКИ РЕШЕНИЙ С ОТКРЫТЫМ КОДОМ В ЗАКОНЕ ЕС ОБ ИИ (AI ACT)

GitHub, Hugging Face, Creative Commons и ряд неназванных организаций призывают усилить поддержку разработки различных моделей ИИ с открытым кодом при рассмотрении вопроса об окончательном принятии закона.

В списке предложений, направленных в Европарламент в преддверии окончательного принятия законопроекта, – более четкие определения компонентов ИИ, уточнение относительно отсутствия выгоды от ИИ для исследователей, работающих над моделями по открытой лицензии, разрешение ограниченного тестирования проектов ИИ в реальных условиях и установление пропорциональных требований для различных моделей.

GARTNER ОПУБЛИКОВАЛ РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ ПОДХОДОВ К ОЦЕНКЕ ИНВЕСТИЦИЙ В ИИ ЗА 2022 ГОД

При оценке показателя окупаемости инвестиций (ROI) в ИИ, 52% организаций, достигших зрелости в этой области, ориентируются на сочетание технических и бизнес-показателей. В менее зрелых организациях чаще используются только технические показатели.

41% компаний используют для оценки ROI бизнес-показатели, связанные с успешностью клиентов. Кроме того, 47% организаций называют обслуживание клиентов одной из трех основных бизнес-функций, получающих выгоду от применения ИИ.

Исследование также показало, что 55% организаций, ранее внедрявших ИИ, всегда рассматривают ИИ для каждого нового кейса применения, который они оценивают. Более половины организаций (52%) отмечают, что факторы риска являются критически важными при оценке новых сценариев использования ИИ.

Опрос проводился с октября по декабрь 2022 года среди 622 респондентов-организаций США, Франции, Великобритании и Германии.

CAPGEMINI ОПУБЛИКОВАЛ ОТЧЕТ «ПРИМЕНЕНИЕ ГЕНЕРАТИВНОГО ИИ: ПЕРЕДОВЫЕ ОТРАСЛЕВЫЕ КЕЙСЫ»

По результатам глобального исследования, 21% опрошенных руководителей утверждают, что генеративный ИИ значительно изменит их отрасли, а 74% заявляют, что выгоды от применения генеративного ИИ перевешивают риски.

74% руководителей компаний сектора высоких технологий утверждают, что создали специальные группы и выделили бюджеты на генеративный ИИ. В сфере финансовых услуг этот показатель составляет 42%. Треть руководителей финансовой отрасли заявляют, что используют генеративный ИИ для создания синтетических данных.

В разрезе финансовых услуг ТОП-3 кейса пилотирования генеративного ИИ – подготовка финансовой отчетности (38%), обнаружение мошенничества (34%), а также прогнозирование денежных потоков (32%). Промышленная эксплуатация технологии по вышеуказанным направлениям пока не превышает 5%.

МЕЖДУНАРОДНЫЙ ВАЛЮТНЫЙ ФОНД (МВФ) ОПУБЛИКОВАЛ 2 ОТЧЕТА, ПОСВЯЩЕННЫХ СОЦИАЛЬНЫМ АСПЕКТАМ И КОНФИДЕНЦИАЛЬНОСТИ В МЕТАВСЕЛЕННОЙ

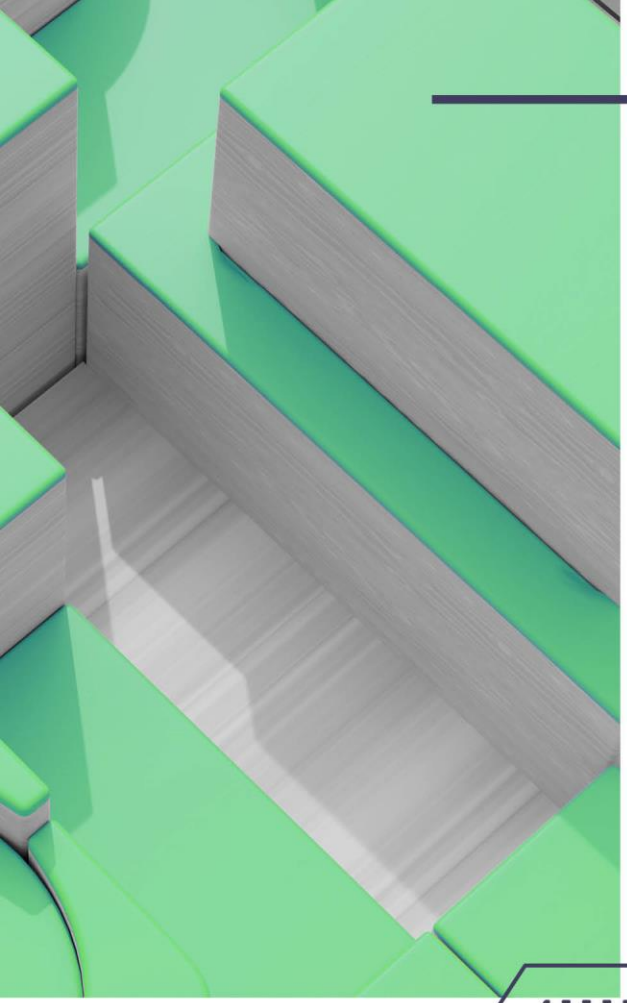
Согласно прогнозам аналитиков МВФ, в ближайшие три года объем рынка метавселенной достигнет $1 трлн. Это будет обусловлено быстрым распространением таких технологий, как генеративный ИИ. В отчете «Конфиденциальность и безопасность в метавселенной» подчеркивается необходимость всемирного сотрудничества стейкхолдеров для развития понимания метавселенной и выработки защитных мероприятий. В сопроводительном выпуске «Социальные аспекты метавселенной» представлено целостное понимание влияния метавселенной на людей, экономику и общество.

БОЛЕЕ 160 ТЕХНОЛОГИЧЕСКИХ КОМПАНИЙ ПРИЗВАЛИ ЕС ТЩАТЕЛЬНО ПРОДУМАТЬ РЕГУЛИРОВАНИЕ ИИ

Компании опубликовали открытое письмо против предложенного европейского Закона об искусственном интеллекте (AI Act), заявив, что он потенциально угрожает конкурентоспособности и инновационности региона. В письме предупреждается, что правила приведут к жесткому регулированию инструментов генеративного ИИ и повлекут как риски ответственности, так и высокие затраты на соблюдение требований для компаний, разрабатывающих эти технологии.

МЕТА (ЗАПРЕЩЕНА В РФ) И MICROSOFT АНОНСИРОВАЛИ ЗАПУСК БОЛЬШОЙ ЯЗЫКОВОЙ МОДЕЛИ (LLM) ПО ОТКРЫТОЙ ЛИЦЕНЗИИ LLAMA-2

Модель будет использоваться на базе облачной вычислительной платформы Azure от Microsoft. LLaMa-2 на 70B параметров сравнима по качеству с GPT-3.5 и превосходит ее по некоторым бенчмаркам. LLaMa 2 бесплатна для исследований и коммерческого использования, а также оптимизирована для работы на Windows.



АССОЦИАЦИЯ ФИНТЕХ ИССЛЕДОВАНИЯ И АНАЛИТИКА

МАРИАННА ДАНИЛИНА
Руководитель Управления исследований и аналитики
E: m.danilina@fintechru.org

ДАРЬЯ ПЕТРОВА
Ведущий бизнес-аналитик по исследовательской деятельности
E: d.petrova@fintechru.org

ГРИГОРИЙ КАРУНАС
Бизнес-аналитик по информационным сервисам
E: g.karunas@fintechru.org

TELEGRAM КАНАЛ

WWW.FINTECHRU.ORG