SOLAR

ТРЕНИРОВКИ ПО ЗАЩИТЕ ОТ КИБЕРУГРОЗ: РОССИЙСКАЯ ПРАКТИКА

Исследование

Содержание

О компании

Группа компаний «Солар» — ведущий поставщик решений кибербезопасности в России, архитектор комплексной кибербезопасности. Ключевые направления деятельности — аутсорсинг ИБ, разработка собственных продуктов, обучение ИБ-специалистов, аналитика и исследование киберинцидентов.

С 2015 года предоставляет ИБ-решения организациям от малого бизнеса до крупнейших предприятий ключевых отраслей. Продукты и сервисы «Солара» объединены в домены экспертизы: Безопасная разработка программного обеспечения, Управление доступом, Защита корпоративных данных, Детектирование угроз и хакерских атак. Домены экспертизы закрывают все потребности заказчиков и включают собственные разработки, решения партнеров, услуги по созданию стратегии и архитектуры ИБ, консалтинг, обучение персонала.

Компания предлагает сервисы первого и крупнейшего в России коммерческого SOC — Solar JSOC, экосистему управляемых сервисов ИБ — Solar MSS. Линейка собственных продуктов включает DLP-решение Solar Dozor, шлюз веб-безопасности Solar webProxy, межсетевой экран нового поколения Solar NGFW, IdM-систему Solar inRights, PAM-систему Solar SafeInspect, анализатор кода Solar appScreener и другие.

Работа центра исследования киберугроз Solar 4RAYS нацелена на изучение тактик киберпреступников. Полученные аналитические данные обогащают разработки Центра технологий кибербезопасности.

Для проведения киберучений и построения киберполигонов применяется платформа «Солар Кибермир», которая постоянно развивается с учетом новых видов угроз. Для комплексного развития навыков кибербезопасности ИБ-специалистов предлагается программа Solar CyberBoost.

Совместно с Минцифры реализуется всероссийская программа кибергигиены, направленная на повышение цифровой грамотности населения.

Подразделения «Солара» расположены в Москве, Санкт-Петербурге, Нижнем Новгороде, Самаре, Ростове-на-Дону, Томске, Хабаровске и Ижевске. Технологии компании и наличие распределенных по всей стране центров компетенций позволяют ей работать в режиме 24/7.

более

850

крупнейших компаний России под защитой «Солара»

более

1800

специалистов — штат компании

Продукты киберполигона «Солар»

Киберучения

- Командно-штабные тренировки для организационной отработки сценариев реагирования
- Практические киберучения для проверки навыков защиты от киберугроз для технических специалистов: стандартные и кастомные

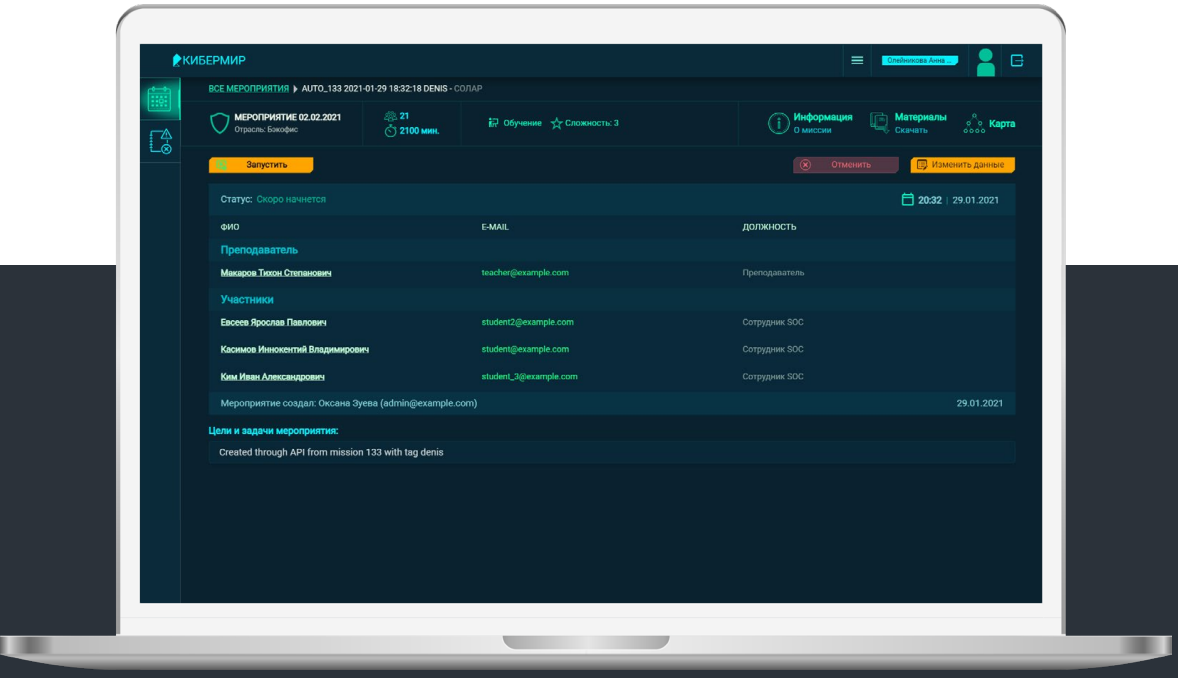
Построение киберполигонов

- Построение киберполигонов на базе инфраструктуры заказчика с использованием платформы «Солар Кибермир»
- Создание цифровых двойников сегментов ИТ-инфраструктуры заказчика на базе мощностей киберполигона от «Солар»

Программа развития навыков кибербезопасности Solar CyberBoost

- Модульный киберинтенсив для получения ключевых знаний и навыков ИБ
- Комплексная программа развития навыков киберзащиты для Blue Team, практическая отработка на киберполигоне

Программная платформа «Солар Кибермир» лежит в основе всех продуктов киберполигона «Солар» для организации киберучений, построения киберполигонов и развития навыков кибербезопасности.



Программная платформа «Солар Кибермир» лежит в основе всех продуктов киберполигона «Солар» для организации киберучений, построения киберполигонов и развития навыков кибербезопасности.

Введение

Устойчивый рост количества кибератак и повышение уровня их сложности требует от специалистов по кибербезопасности регулярного совершенствования компетенций по противостоянию злоумышленникам. Тренироваться выявлять и отражать кибератаки без риска реального ущерба для предприятия позволяют киберполигоны — цифровые двойники типовой инфраструктуры, на которых эмулируются процессы организаций.

Эксперты «Солар» провели исследование с целью выяснить, как российские компании относятся к кибертренировкам, определить долю тех, кто имеет опыт участия в таких проектах, и тех, кто только планирует проводить киберучения в будущем.

Авторы исследования выяснили:

- какие бюджеты организации готовы выделять на кибертренировки
- сколько сотрудников они планируют тренировать в рамках учений
- с какой периодичностью считают необходимым проводить киберучения

Кроме того, эксперты выделили основные факторы, которые мешают российским организациям проводить для своих сотрудников тренировки по защите от киберугроз.

Методология

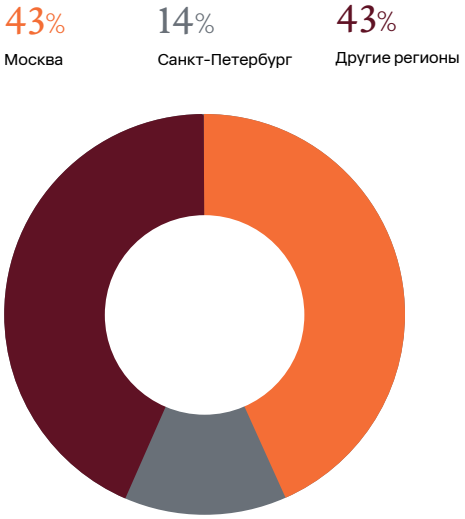
Данное исследование проведено методом количественного онлайн-опроса, в котором приняли участие порядка 100 представителей различных российских организаций, отвечающих за выбор и внедрение продуктов и сервисов по кибербезопасности.

В число респондентов вошли коммерческие компании и организации государственного сектора, включая федеральные и региональные органы власти. В опросе принимали участие представители различных сегментов бизнеса: B2G, B2E, B2B, B2SMB.

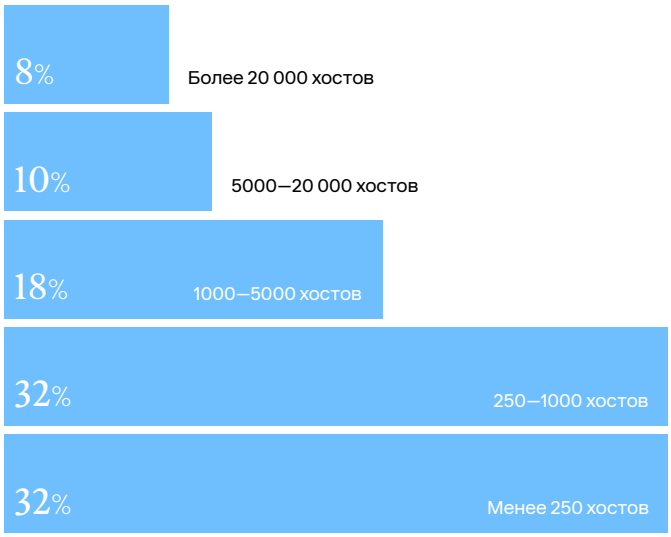
География участников исследования охватывает Москву и Санкт-Петербург, а также другие регионы страны. В ходе опроса респондентам предлагалось выбрать один или несколько из предложенных вариантов ответа.

Должности респондентов

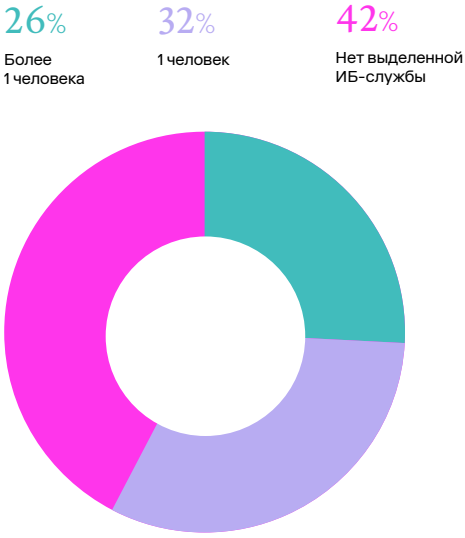
География



Размер организации по количеству хостов



Размер ИБ-службы



Ключевые цифры

52%

Каждая вторая российская организация (52%) заявляет об опыте участия в киберучениях, а три четверти компаний (75%) планируют проведение таких проектов в будущем.

500 тыс. рублей

Примерно 68% компаний, планирующих проведение киберучений, готовы потратить до 500 тысяч рублей на тренировки одного сотрудника в год.

59%

Почти в 59% компаний работает не более 10 сотрудникам, которым необходимы тренировки навыков защиты от киберугроз.

87%

В большинстве компаний (87%) считают, что киберучения необходимо проводить как минимум каждые полгода.

Результаты исследования

Насколько широко киберучения распространены в России

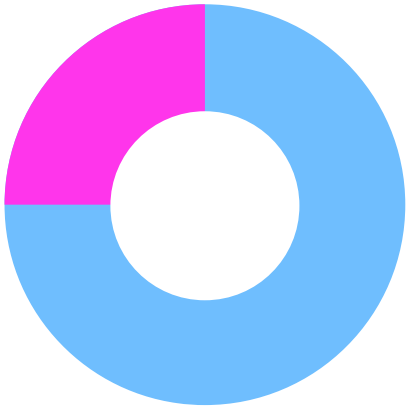
В рамках исследования эксперты «Солар» выяснили, какова доля компаний, которые уже имеют опыт участия в киберучениях и которые только планируют проводить их в ближайшие три года. Как показали результаты опроса, около половины организаций (52% респондентов) принимали участие в киберучениях ранее и три четверти компаний (75% опрошенных) планируют провести их в будущем.

Участвовала ли ваша компания в киберучениях?

52%
Да

48%
Нет

Планирует ли ваша компания проводить киберучения для сотрудников?



75%
Да

25%
Нет

75%

опрошенных планируют провести киберучения в будущем

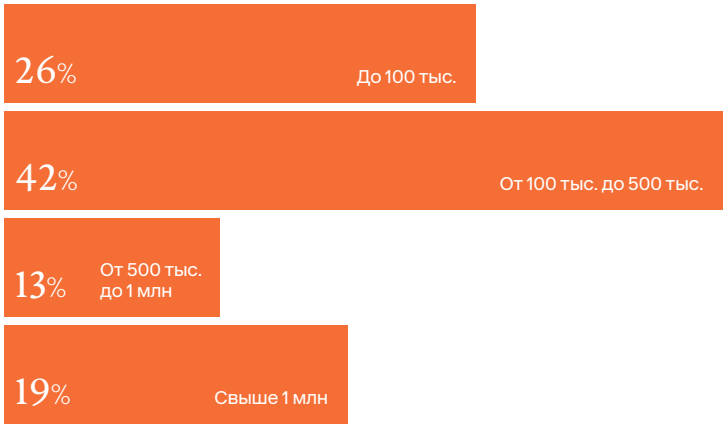
Сколько компании готовы тратить на киберучения

Респондентам, заявившим о планах принять участие в киберучениях, предлагалось оценить примерный бюджет, который компания готова потратить на кибертренировки одного сотрудника в год.

Примерно каждый четвертый опрошенный (26%) отметил, что бюджет на эти цели может составлять до 100 тысяч рублей, и еще почти 42% заявили о готовности компании выделять на кибертренировки одного сотрудника от 100 до 500 тысяч рублей в год.

При этом почти треть компаний (32%), планирующих проведение таких проектов, готовы инвестировать в кибертренировки одного сотрудника свыше полумиллиона рублей.

Сколько ваша компания готова тратить на киберучения одного сотрудника в год? (руб.)



42%

компаний готовы инвестировать в киберучения одного сотрудника в год от 100 до 500 тыс. рублей

Сколько сотрудников планируют тренировать компании на киберучениях

Также эксперты «Солар» выяснили численность сотрудников, для которых компании планируют проводить киберучения. Около 22% опрошенных отметили, что в киберучениях смогут принять участие один-два сотрудника, еще почти 37% планируют провести кибертренировки для трех-десяти сотрудников.

Таким образом, из данных опроса следует, что почти в 59% компаний работает не более 10 сотрудников, которым необходимы тренировки навыков защиты от киберугроз.

Также почти каждый пятый (22%) заявил, что киберучения могут быть рассчитаны на десять-пятьдесят сотрудников.

Сколько сотрудников будет участвовать в киберучениях (при наличии планов их проведения)?

37%

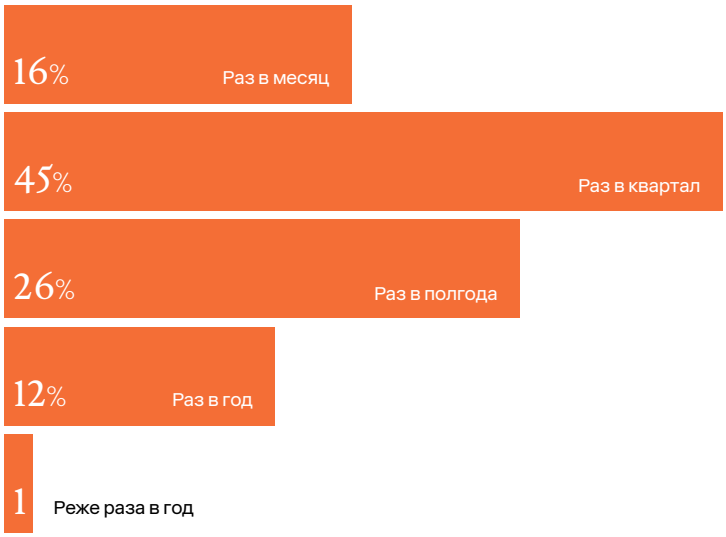
компаний планируют провести кибертренировки для 3–10 сотрудников

С какой периодичностью нужно проводить киберучения

Примерно 45% опрошенных из тех, кто планирует проведение киберучений, отмечают, что для получения реального эффекта такие проекты следует реализовывать как минимум раз в квартал, и еще порядка 26% заявляют о необходимости их проведения раз в полгода.

О меньшей периодичности — раз в год и реже — заявляют суммарно 13% респондентов.

Как часто необходимо проводить практические тренировки по отражению кибератак для получения реального эффекта от киберучений?



45%

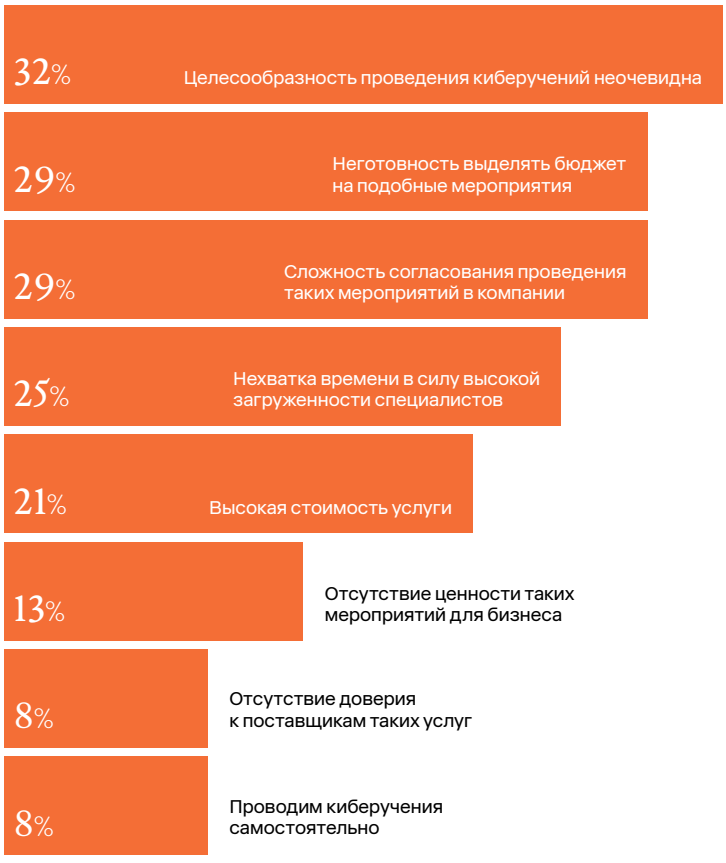
компаний планируют проведение киберучений раз в квартал

Распространенные барьеры, препятствующие проведению киберучений

Респондентам, которые заявили об отсутствии планов участвовать в киберучениях, в ходе исследования предлагалось назвать основные факторы, сдерживающие реализацию таких проектов. При этом можно было выбрать несколько вариантов ответа и предложить собственный.

Как показали результаты опроса, барьерами, препятствующими проведению киберучений, респонденты считают неочевидность целесообразности проведения киберучений (32%), отсутствие бюджетов (29%), сложности согласования таких мероприятий в компании (29%), нехватку времени специалистов из-за их высокой загруженности (25%) и высокую стоимость услуги по организации киберучений (21%).

Что для вас служит сдерживающим фактором при принятии решения об участии в киберучениях?



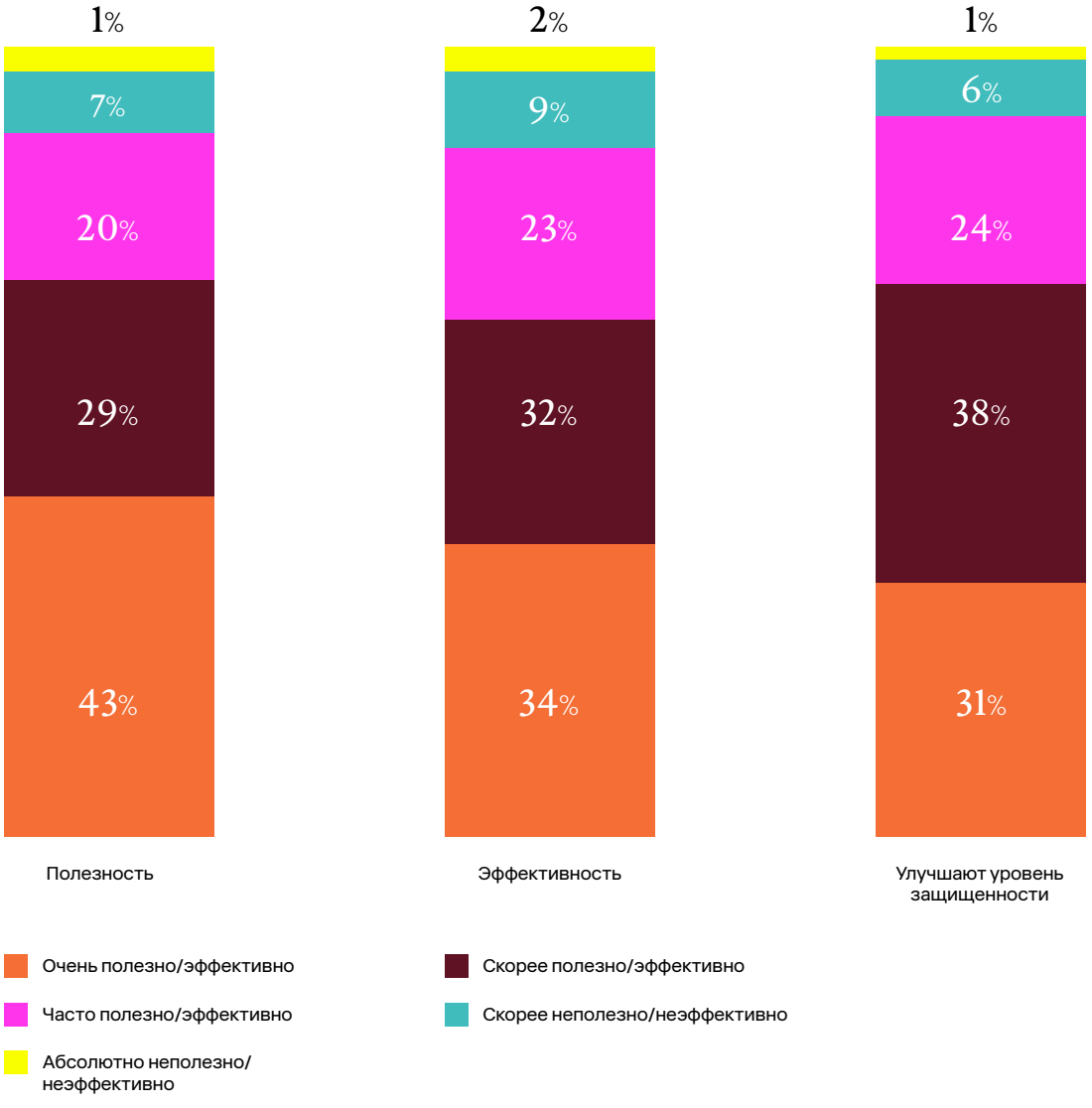
32%

не осознают целесообразности проведения киберучений

Оценка полезности и эффективности киберучений

Эксперты «Солар» выяснили, как российские организации в целом оценивают полезность и эффективность киберучений. Большинство респондентов отметили, что считают кибертренировки полезными (72%) и эффективными (66%).

Также 69% опрошенных считают, что киберучения помогают повысить уровень защищенности организации. При этом респонденты из крупных компаний видят в киберучениях больше ценности, чем из небольших.



Выводы

Как видно из результатов исследования:

- большинство компаний считают киберучения полезным и эффективным инструментом для повышения уровня защищенности от киберугроз;
- многие компании уже имеют опыт участия в кибертренировках и планируют их проведение в будущем;
- компании осознают необходимость регулярных тренировок и их реальную пользу для формирования устойчивого навыка защиты от кибератак.

Часть компаний пока присматривается к киберучениям, что неудивительно, поскольку рынок киберучений в России начал формироваться относительно недавно по сравнению с зарубежным: сейчас наблюдается его активный рост, расширяется количество коммерческих предложений, появляются лучшие практики. Должно пройти некоторое время для осознания компаниями ценности киберучений и повышения степени их готовности к использованию этого инструмента.

Весомую роль в развитии практики проведения киберучений в России играет создание тренировочной площадки киберполигона «Солар» для будущих и действующих специалистов по кибербезопасности. С 2020 по 2022 год на киберполигоне «Солар» было проведено более 250 киберучений и обучено более 3000 специалистов по информационной безопасности. В 2023 году прогнозируется двукратное увеличение количества киберучений для организаций за счет актуализации темы повышения квалификации сотрудников для противостояния современным киберугрозам.

W:
cybermir.ru
rt-solar.ru
rt.ru

T:
+7 (499) 755-07-70 — продажи и общие вопросы
+7 (499) 755-02-20 — техническая поддержка

E:
cybermir@rt-solar.ru
pr@rt-solar.ru

A:
г. Москва, Никитский пер., д. 7, стр. 1

SOLAR