РБК+

ТЕМАТИЧЕСКОЕ ПРИЛОЖЕНИЕ К ЕЖЕДНЕВНОЙ ДЕЛОВОЙ ГАЗЕТЕ РБК

Вторник, 23 ноября 2021 | № 177 (3466)

Инструменты

Почему сервисы информационной безопасности эффективнее опоры на собственные силы

→ 4

Кибербезопасность

ТЕНДЕНЦИИ | **Число кибератак увереннно растет**

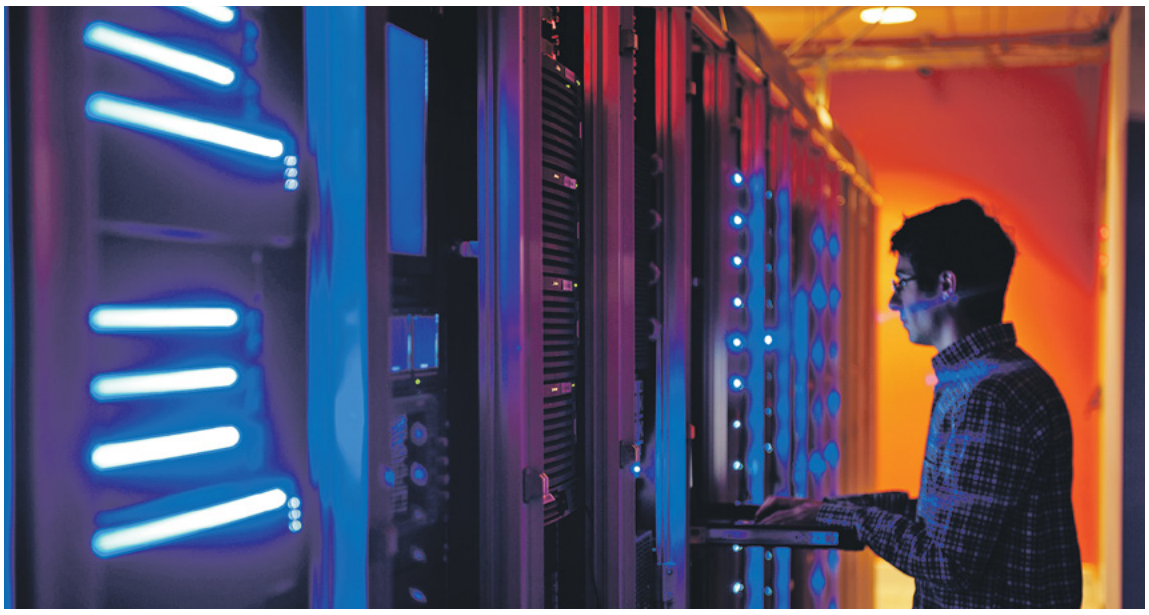
Пандемия COVID-19 запустила новую **ВОЛНУ** *угроз на рынке кибербезопасности. Переход на* **УДАЛЕННУЮ** *работу и бум цифровых сервисов* **МОБИЛИЗОВАЛИ** *киберпреступников.*

Бизнес под ударом: как защитить компанию от киберугроз

Фото: Getty Images Russia

→ 2

Тенденции



Компаниям необходимо постоянно совершенствовать свою инфраструктуру безопасности, используя современные комплексные защитные решения

1

МАРИЯ ПОПОВА

По оценкам Всемирного экономического форума (ВЭФ), глобальные потери от киберпреступлений, совершаемых против государственных организаций, коммерческих предприятий и отдельных граждан, составляют $600 млрд в год. Этот показатель постоянно растет и, по прогнозам ВЭФ, составит $5,2 трлн суммарно за период 2019–2023 годов. «Это сделает киберпреступления одним из наиболее разрушительных для глобальной экономики типом преступлений», — отмечает менеджер практики кибербезопасности и непрерывности бизнеса PwC в России Михаил Толчельников.

Количество инцидентов, регистрируемых в 2021 году центром мониторинга кибератак компании «Информзащита», выросло более чем в полтора раза по сравнению с аналогичным периодом 2020 года. «Растет не только уровень сложности атак, но и их скорость, тенденция будет сохраняться соразмерно темпу цифровизации организаций и повсеместного внедрения и развития технологий», — отмечает директор центра противодействия кибератакам компании «Информзащита»

Согласно результатам международного исследования консалтинговой компании EY по информационной безопасности за 2021 год, 81% респондентов-руководителей отмечают, что из-за пандемии COVID-19 и бюджетных ограничений компании не уделяют должного внимания управлению киберрисками. Существенный рост числа киберугроз и последствий от их реализации связан с повсеместным распространением удаленного или гибридного форматов работы. «В период пандемии структурные подразделения ИТ и информационной безопасности (ИБ) фокусировались в большей степени на увеличении существующих мощностей и масштабируемости компонентов ИТ-инфраструктуры, развитии ландшафта технических средств и выборе новых, зачастую нестандартных, инструментов коллаборации», — поясняет директор практики консалтинга, услуг в области управления рисками ИТ и кибербезопасности EY Андрей Абашев. На этом фоне хакерские атаки становились более изощренными, а достигаемый негативный эффект распространяется теперь уже не только на компанию-жертву, но и на всю цепочку поставок или экосистему, частью которой она является.

В «Лаборатории Касперского» также отмечают рост числа кибератак за последнее время. Здесь ежедневно обнаруживают до 350 тыс. новых образцов вредоносных программ, и этот показатель продолжает расти. В числе наиболее дорогостоящих для крупного бизнеса киберинцидентов — электронные утечки данных из внутренних систем, целевые атаки, утечки, вызванные атаками вредоносного ПО на мобильные устройства сотрудников или произошедшие вследствие физической их потери. А для малого и среднего бизнеса наиболее дорогостоящими в 2021 году, по данным «Лаборатории Касперского», стали инциденты, вызванные несоблюдением внутренних ИБ-политик, атаки вирусов-майнеров, инциденты на стороне партнеров, с которыми компания обменивается информацией, а также атаки на филиалы.

По мнению более чем 60% респондентов, опрошенных PwC в рамках исследования 2022 Global Digital Trust Insights Survey, число киберпреступлений продолжит расти. «Предполагается, что основными мишенями станут мобильные устройства, интернет вещей, облачные сервисы. При этом также можно ожидать существенного роста атак на цепочки поставок, включая технологические поставки и ПО», — считает Михаил Толчельников.

ПРОБЛЕМНЫЕ ЗОНЫ

В центре мониторинга «Информзащиты» фиксируют в настоящий момент три основных тренда, связанных с киберрисками, — промышленный шпионаж (18% от общего количества инцидентов), программы-вымогатели (27%) и майнеры криптовалюты (36%). Самые серьезные последствия и сложные техники атак демонстрируют APT-группировки при попытках шпионажа, направленного на крупные промышленные предприятия и госсектор. «Растет активность программ-вымогателей, набирает обороты так называемый Big Game Hunting — атаки на крупные компании в целях получения выкупа, появляются коллаборации кибергруппировок», — перечисляет Иван Мелехин.

По словам Михаила Толчельникова, злоумышленники продолжат держать в фокусе атак предприятия финансовой сферы, а также организации с высокой степенью зависимости от доступности их цифровых сервисов или наличием существенного объема интеллектуальной собственности. Среди основных методов воздействия — повреждение цифровой инфраструктуры, захват вычислительных мощностей, разрушение цепочки поставок и создание потоков дезинформации.

«Стоит разделить кибермошенничество по типам мотивации: коммерческие кибератаки в целях наживы (составляют подавляющее большинство), а также более редкие и сложные целевые атаки и кибершпионаж», — поясняет управляющий директор по России и СНГ «Лаборатории Касперского» Михаил Прибочий. В первом случае отрасль для мошенников не играет роли: чем крупнее компания и чем более уязвима ее система безопасности, тем больше у нее шансов стать жертвой кибератаки. Во втором — злоумышленников интересуют государственные структуры, научно-исследовательские и конструкторские предприятия, объекты критической инфраструктуры, крупные центры хранения и обработки данных, военные объекты. При этом количественно эти атаки занимают единицы процентов от всего объема киберугроз.

ВОЗМОЖНОСТИ ЗАЩИТЫ

По результатам проведенного EY в 2021 году международного опроса директоров по рискам, лишь 9% респондентов уверены в том, что существующие в их организации меры по минимизации киберрисков способны защитить от серьезных кибератак (по сравнению с 20% в 2020 году). 58% опрошенных заявили, что их компания внедряет новые технологии в сроки, которые не позволяют провести надлежащую оценку киберрисков или осуществлять эффективный надзор за ними.

Усилить устойчивость бизнеса по отношению к киберугрозам поможет развитие риск-ориентированной культуры, повышение зрелости функции управления киберрисками, а также установление прозрачной коммуникации как между советом директоров и службой киберзащиты, так и при взаимодействии с бизнес-партнерами и третьими лицами, включенными в цифровую платформу компании, считает Михаил Толчельников.

Компаниям необходимо постоянно укреплять и совершенствовать свою инфраструктуру безопасности, используя современные комплексные защитные решения, отмечает Михаил Прибочий: «В числе таких решений, к примеру, сервисы безопасного доступа, с помощью которых можно собирать данные телеметрии из сетевого трафика, останавливать атаки в периметре и сети». Также, по мнению эксперта, важно развернуть расширенную систему обнаружения и устранения угроз, которая сможет в автоматическом режиме реагировать на инциденты на всех конечных устройствах.

Приобретением любого количества продуктов для кибербезопасности в настоящее время защититься от атак практически невозможно. В первую очередь необходимы высококвалифицированные специалисты, способные выявлять атаки и противостоять хакерам, дополняет Иван Мелехин. Здесь, по его мнению, для большинства организаций наиболее простым выходом будет обратиться к MSSP-провайдерам, которые в рамках сервисной модели предоставляют необходимые продукты и услуги квалифицированного персонала.

«Применение подхода, когда служба информационной безопасности является одним из ключевых участников этапа планирования бизнес-инициатив, позволяет заранее продумать элементы контрольной среды, а использование концепции нулевого доверия существенно повысит уровень кибербезопасности при взаимодействии информационных систем как внутри компании, так и с системами других участников цепочки поставок», — резюмирует Андрей Абашев.

$600 млрд
в год составляют потери от киберпреступлений в мире, по оценке Всемирного экономического форума

Фото: Getty Images Russia

От первого лица

«Киберпреступность и кибербезопасность — классическая игра в погоню»

О роли страхования в вопросе кибербезопасности бизнеса **РБК+** рассказал директор по рискам **«СБЕРСТРАХОВАНИЯ»** ВЛАДИМИР НОВИКОВ.

Фото: пресс-служба

Насколько сегодня в целом актуальны вопросы кибербезопасности для бизнеса?

Киберриски, несомненно, являются одной из главных угроз для бизнеса. Процесс тотальной цифровизации продолжается, и киберпреступления становятся частью повседневной жизни. Бизнес-процессы трансформируются под высокотехнологичное общество и повышают эффективность взаимодействия внутри компаний и между ними. Например, в «цифру» сейчас перешло все взаимодействие с финансовыми учреждениями, с государственными органами.

Но нужно понимать, что помимо новых возможностей цифровизация создает и дополнительные риски. Пандемия стала катализатором перехода в онлайн, что, в свою очередь, расширило поле деятельности для киберпреступников. Однако параллельно стали активнее реализовываться и контрмеры со стороны бизнеса и государства. Киберпреступность и кибербезопасность — это классическая игра, где одни убегают, а другие догоняют.

Что чаще всего становится целью киберпреступников?

В большинстве случаев кибератаки нацелены на кражу денежных средств, коммерческой информации, баз данных, интеллектуальных продуктов.

Какие отрасли подвержены наибольшим рискам?

Сфера бизнеса не так важна: любой предприниматель использует «банк — клиент» и различные электронные системы. Поэтому потенциальный риск кражи денег и данных есть везде. Также возможен сценарий блокировки ключевого рабочего процесса компании вирусом-шифровальщиком с требованием выкупа. К сожалению, в большинстве случаев жертвы решают заплатить кибервымогателям, а не обращаться в правоохранительные органы, страховую компанию или к специалистам по кибербезопасности.

Если говорить о размере бизнеса, то очевидно, что атаковать крупные компании или банки, которые имеют высокий уровень информационной защиты, всегда труднее. Для малых же предприятий — с более слабой защитой — достаточно написать универсальные программы, которыми можно атаковать через фишинговые письма.

Наш опыт показывает, что основным индикатором киберзащищенности бизнеса является реакция компании и ее сотрудников на фишинговые рассылки. Именно поэтому в крупных корпорациях регулярно проводятся киберучения, во время которых рассылаются фейковые письма и производятся замеры, сколько сотрудников их открыли. Примерно таким же образом ведут разведку и преступники, определяя, к какому предприятию легче подступиться.

Как этому явлению противостоять?

Есть два пути. Первый — работать с профессионалами по киберзащите. Второй — застраховаться от киберрисков. Лучше, конечно, сделать это в комплексе, поскольку компании по управлению цифровыми рисками и страховщики решают разные задачи: одни — предупреждают неприятные ситуации, другие — решают проблемы, связанные с их последствиями.

Насколько в России развит сегмент страхования от киберпреступлений?

Ему однозначно есть куда развиваться. В составе Всероссийского союза страховщиков есть рабочая группа по киберстрахованию, которой я руковожу. Пока в нее входят представители лишь 15 страховых компаний более чем из ста зарегистрированных в России.

Во многом такой уровень вовлеченности объясняется тем, что для классического страхования киберинцидент — это не очень понятная вещь. Классическое страхование предполагает, что есть некая статистика для формирования тарифа. В нашем случае ее нет, поэтому мы работаем на основании результатов собственных опросов, исследований консалтинговых компаний, данных компаний по киберзащите. Анализ сводной информации позволяет нам оценить стоимость киберриска.

Кроме того, для занятия киберстрахованием нужно создавать определенную инфраструктуру, чтобы, во-первых, иметь возможность провести расследование страхового случая, а во-вторых, минимизировать его последствия. Получается, что это не совсем страхование, а комбинация с работой по кибербезопасности.

По нашим оценкам, затраты на расследование среднего кейса могут составить от 500 тыс. до 2 млн руб. То есть страховщику нерентабельно содержать в штате опытного следователя. Поэтому мы, в частности, идем по пути партнерства с лидерами рынка киберзащиты — компаниями «Лаборатория Касперского», Bi.Zone и др.

Также в полисах для малого бизнеса мы кроме возмещения прямых убытков предусматриваем компенсацию расходов на таких специалистов. Для крупного бизнеса это обычно не так актуально, хотя у них тоже есть соответствующая опция.

Что предлагает ваша компания и насколько ваши продукты затратны для бизнеса?

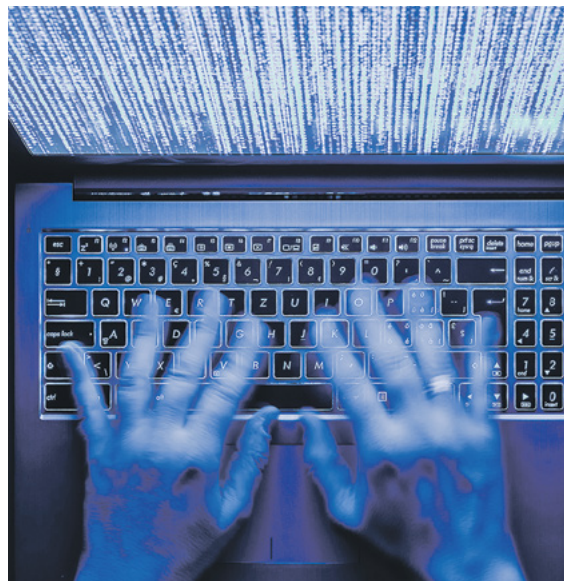
У нас есть серия продуктов «Мое киберстрахование Оптима». Она предусматривает страховую защиту от основных актуальных угроз: потери данных или информационных систем, перерыва в производстве, кражи финансовых активов, а также страхование гражданской ответственности и дополнительных расходов на расследование и восстановление данных. Сейчас продукт представляет собой конструктор, где клиент может самостоятельно выбирать опции. Страховое покрытие при этом может составить от 1,5 млн до 10 млн руб.

> «Основным индикатором киберзащищенности бизнеса является реакция компании и ее сотрудников на фишинговые рассылки»

Инструменты

Цифровой щит: кто в ответе за сервисы информационной безопасности

Сложность и динамика киберугроз постоянно возрастают. Эффективно противостоять кибератакам помогают ИБ-решения по сервисной модели от внешних провайдеров.



Защита цифрового периметра компании похожа на бесконечную игру: как только одна уязвимость закрыта, сразу же возникает новая

Фото: Getty Images Russia

МАРИЯ ПОПОВА

Согласно результатам международного исследования EY по информационной безопасности, дестабилизация, вызванная пандемией коронавируса, создала условия для существенного роста кибератак и утечек данных. За последний год многие организации внедрили новые технологии и облачные инструменты, чтобы обеспечить удаленную работу, однако в развивающуюся корпоративную среду начали проникать новые уязвимости. Три четверти (77%) респондентов GISS сообщили о росте количества серьезных кибератак, в том числе с помощью программ-вымогателей, за последние 12 месяцев.

Атаки киберпреступников становятся более масштабными, а их тактика — все более непредсказуемой. По данным исследования FortiGuard Labs, цепочка поставок киберпреступности за последний год резко выросла и лишь менее 0,05% киберпреступников арестовываются и привлекаются к ответственности. В EY отмечают, что злоумышленники все чаще используют новые стратегии — совершают фишинговые атаки с применением вредоносных программ, которые пересылаются сотрудниками, или добавляют бэкдор, позволяющий использовать коммерческое программное обеспечение после его приобретения клиентами. Менее половины (47%) опрошенных GISS заявили, что они понимают и могут предвосхищать стратегии, которые используют хакеры.

Чтобы обезопасить себя от киберинцидентов, бизнесу необходимо постоянно совершенствовать свою инфраструктуру безопасности. «После событий 2020–2021 годов компании осознали, что отсутствие комплексного подхода к обеспечению информационной безопасности может критически отразиться как на прибыли, так и на репутации бренда», — отмечает руководитель службы информационной безопасности компании «Онланта» (входит в группу ЛАНИТ) Мурад Мустафаев. По его словам, защита цифрового периметра компании похожа на бесконечную игру: как только одна уязвимость закрыта, сразу же возникает новая.

ИБ НА АУТСОРСИНГ

Далеко не все компании готовы формировать отдельный штат специалистов службы информационной безопасности (ИБ) или расширять существующий. «Часть задач по обеспечению информационной безопасности отдают на аутсорсинг, сервис-провайдерам, которые предлагают комплексную модель защиты бизнеса», — комментирует Мурад Мустафаев. Если компания использует как on-premise, так и виртуальную инфраструктуру, то защита должна быть обеспечена на всех уровнях.

На создание собственной комплексной киберзащиты требуется от четырех до шести месяцев, а иногда и больше. Аутсорсинг же сокращает этот срок до нескольких недель. Сервис-провайдер обеспечивает защиту в режиме 24/7, оперативно обновляя политики безопасности сразу, как только становится известно об очередной киберугрозе. «Опираясь на свою базу знаний и опыт работы на разных проектах, поставщики ИБ-решений всегда осведомлены об актуальных отраслевых и законодательных изменениях, сервис-провайдер может оперативно определить класс используемых компанией информационных систем и обрабатываемых данных», — отмечает Мурад Мустафаев. А обширная партнерская сеть с вендорами позволяет подобрать решение под конкретные особенности инфраструктуры заказчика и сделать проект под ключ, добавляет он.

Среди преимуществ в случае выбора внешнего поставщика ИБ — скорость реализации услуги, отмечает заместитель директора центра противодействия кибератакам Solar JSOC компании «Ростелеком» Алексей Павлов. Это связано с тем, что процесс подключения к сервису хорошо отработан, заранее известны подводные камни и их удается обойти. По данным «Ростелекома», среднее время подключения сервисов по ИБ составляет один месяц, при этом интеграционный проект, реализуемый заказчиком самостоятельно, редко выполняется быстрее, чем за полгода.

«Основное преимущество такого подхода для заказчика — простое и быстрое подключение своих информационных систем к готовой инфраструктуре с налаженными процессами и подготовленными кадрами», — комментирует директор центра информационной безопасности компании «ЛАНИТ-Интеграция» (входит в группу ЛАНИТ) Николай Фокин. Каждая из этих составляющих требует значительных временных и финансовых вложений для самостоятельного развития на своей площадке.

Сервисы экономически эффективнее — это операционные затраты, а не капитальные. Заказчик получает выбранные технологии в необходимом именно ему объеме, при необходимости сервисы можно быстро масштабировать или, напротив, сократить до минимума. Бизнесу не нужно тратиться на создание собственной ИБ-инфраструктуры и ее обслуживание. «Управление инструментами информационной безопасности по такой модели позволяет получить все необходимые решения в едином окне — защиту от несанкционированного проникновения злоумышленников в ИТ-системы, защиту от сетевых угроз, защиту веб-приложений и корпоративной почты, централизованную антивирусную защиту, защищенное хранение данных, а также обеспечение соответствия информационных систем заказчика законодательным требованиям в области ИБ», — поясняет Мурад Мустафаев.

Растет востребованность таких услуг, как аудит ИБ и PenTest (тестирование на проникновение), — на основе получаемых при анализе данных можно определить «слепые» зоны, устранить их и сформировать стратегию защиты. В «Ростелекоме» отмечают рост спроса на инфраструктурные сервисы — средства защиты информации (СЗИ) в аренду, сервисы повышения осведомленности и комплексные сервисы по защите от внешних угроз и злоумышленников. По-прежнему актуально обеспечение соответствия информационных систем требованиям регуляторов по хранению и обработке персональных данных по ФЗ-152.

КАДРОВЫЙ ВОПРОС

Спрос на услуги сервис-провайдеров растет в последнее время кратно — на фоне дефицита кадров на рынке ИБ. За счет сервисной модели заказчик может воспользоваться наработанными компетенциями специалистов крупного игрока, который ежедневно отражает сложнейшие кибератаки. «Компании не нужно искать ИБ-специалистов либо заниматься обучением персонала — команда приходит со стороны сервис-провайдера, тем более что некоторых специалистов бессмысленно и невыгодно держать в штате средней компании», — поясняет Алексей Павлов. Например, реверс-инженеры вредоносного ПО, форензеры (специалисты по раскрытию преступлений, связанных с компьютерной информацией), пентестеры (программисты и инженеры, тестирующие уязвимости информационной системы) — все они могут быть привлечены в рамках экспертных сервисов со стороны провайдера услуг.

Но наличие сервис-провайдера не означает, что компания может полностью забыть о ИБ. «Для эффективной киберзащиты необходим совместный подход и разделение зон ответственности между провайдером и штатными специалистами», — считает Алексей Павлов. Например, если провайдер оказывает услуги по мониторингу и выявлению инцидентов, то реагирование на инциденты остается на ИБ-службе заказчика, от которой нужна качественная обратная связь для минимизации ложных срабатываний и адаптации сценариев под конкретную инфраструктуру.

«Некоторые компании опасаются передавать ИБ-процессы на аутсорсинг в связи с риском утечки корпоративных данных, однако при заключении контракта стороны подписывают NDA (соглашение о неразглашении. — РБК), что сводит эти риски к нулю», — говорит Мурад Мустафаев. Многие выбирают гибридные подходы, то есть покупку собственных СЗИ и их передачу в эксплуатацию сервис-провайдерам, дополняет Алексей Павлов.

Николай Фокин отмечает основные сдерживающие факторы — невозможность гибкой конфигурации услуг под каждого заказчика и начальную фазу развития рынка сервисных провайдеров. По его словам, у этой модели есть специфические риски, но положительный эффект от использования таких сервисов больше.

«КИБЕРБЕЗОПАСНОСТЬ» (18+)

Тематическое приложение к «Ежедневной деловой газете РБК»

Является неотъемлемой частью «Ежедневной деловой газеты РБК» № 177 (3466) от 23 ноября 2021 г.

Распространяется в составе газеты

Материалы подготовлены редакцией партнерских проектов РБК+

Партнер проекта: ООО СК «Сбербанк страхование». Реклама

Учредитель: ООО «БизнесПресс»

Издатель: ООО «БизнесПресс»

Директор ИД РБК: Ирина Митрофанова

Главный редактор партнерских проектов РБК+: Наталья Кулакова

Редактор РБК+ «Кибербезопасность»: Владимир Новиков

Выпускающий редактор: Андрей Уткин

Руководитель дизайн-департамента: Николай Реутин

Дизайнеры: Дмитрий Иванов, Сергей Пивоваров

Фоторедактор: Алена Кондюрина

Корректоры: Татьяна Поленова, Маргарита Тарасенко

И.о. главного редактора газеты: Петр Геннадьевич Канаев

Рекламная служба: 8 (495) 363-11-11, доб. 1342

Коммерческий директор издательства РБК: Анна Брук

Директор по продажам РБК+: Евгения Карлина

Директор по производству: Надежда Фомина

Адрес редакции: 115280, Москва, ул. Ленинская Слобода, д. 26, стр. 3