

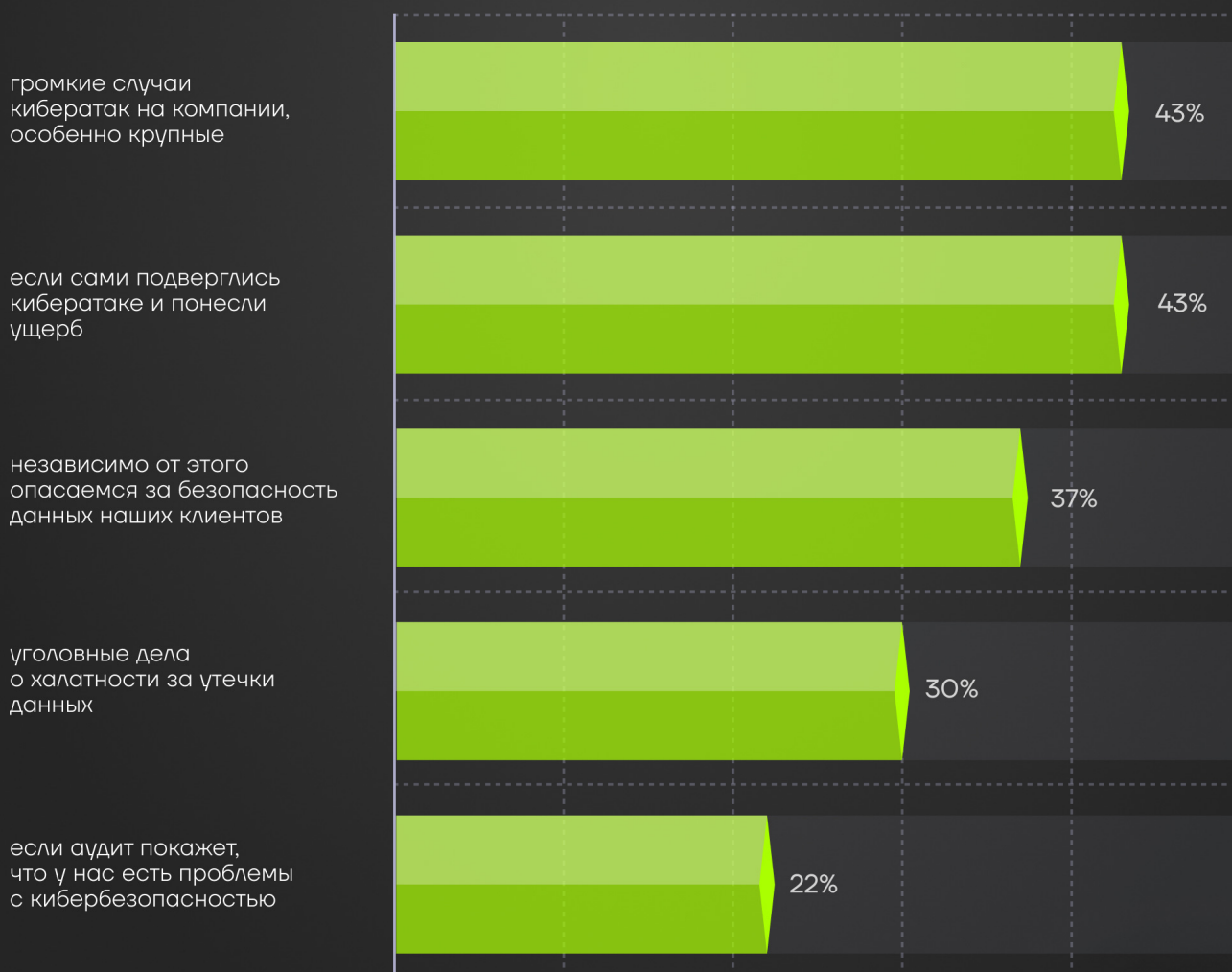


угрозы кибербезопасности и методы защиты малого и среднего бизнеса

Каждый второй предприниматель уверен, что проблема киберугроз для бизнеса становится всё более актуальной. К такому выводу пришли аналитики проекта Кибердом по результатам исследования, проведённого совместно с компанией «Билайн». Исследование показало: 48% предпринимателей считают, что справиться с кибератаками поможет популяризация знаний о кибербезопасности в бизнес-среде, еще 42% ждут больше доступного обучения по кибербезу.

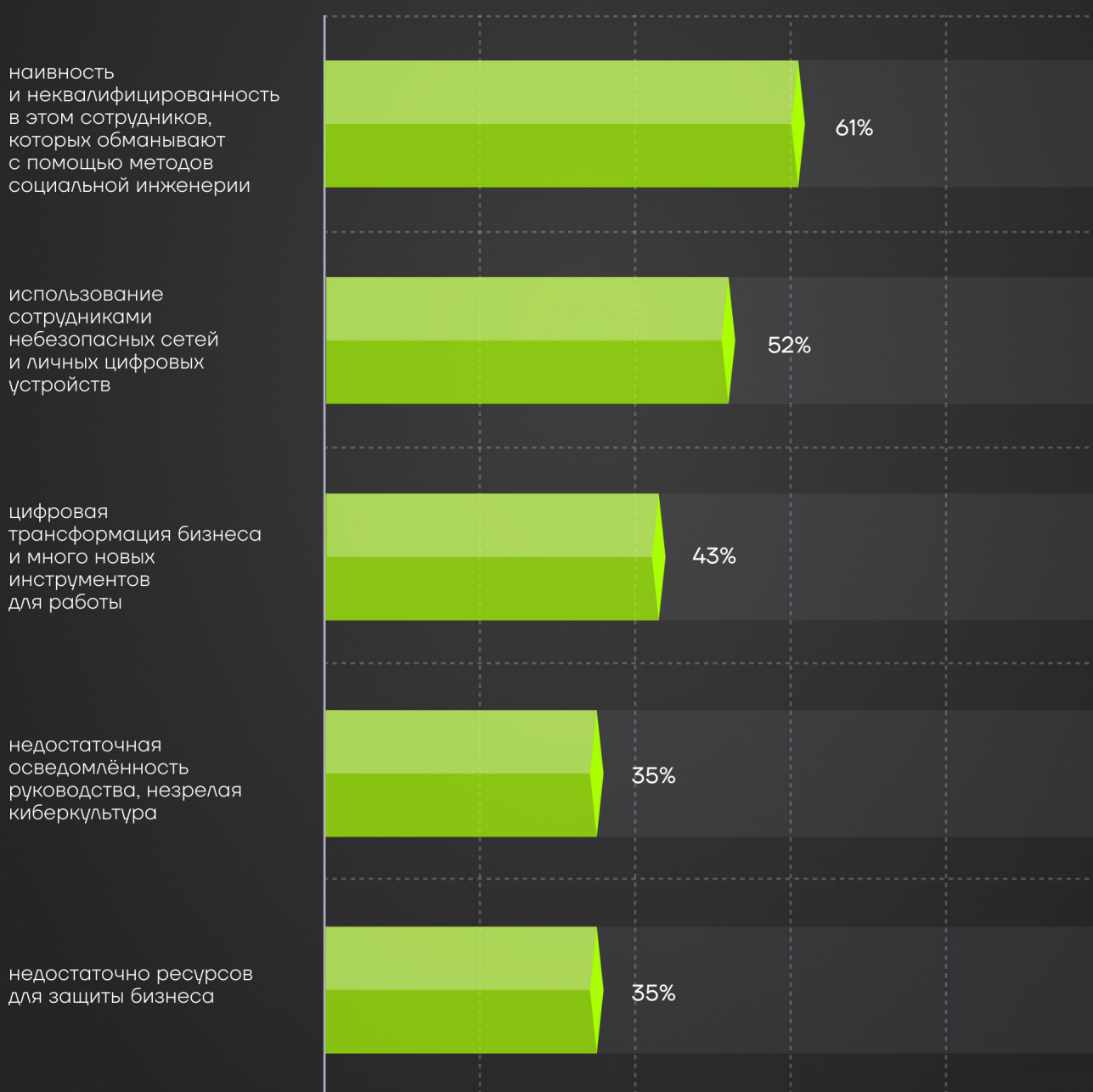
Предприниматели осознают значимость киберугроз для бизнеса, при этом 35% считают, что она осталась на уровне прошлого года, а 20% уверены — в 2026-м опасность только выросла. Киберинциденты — главный драйвер в усилении защиты бизнеса. Так, 43% респондентов отметили, что громкие случаи кибератак на рынке мотивируют их активнее заниматься безопасностью компании. Столько же усиливают кибербезопасность бизнеса, основываясь на собственном опыте, особенно если он сопровождался ущербом. Чуть меньше респондентов (37%) опасаются за безопасность данных своих клиентов, почти треть (30%) напуганы уголовными делами о халатности и утечках данных, а каждый четвёртый представитель бизнеса (22%) полагается на аудит кибербезопасности: наличие угроз мотивирует незамедлительно заняться защитой.

Что мотивирует/мотивировало бы вас заняться кибербезопасностью в компании?



По мнению опрошенных, основная причина атак — низкая киберкультура. Так, 61% отмечают наивность и недостаточную квалификацию сотрудников в этом вопросе, 35% — плохую осведомлённость руководства. Больше половины (52%) считают, что сотрудники сами создают потенциальные угрозы, так как используют личные цифровые устройств и небезопасные сети. Еще 43% респондентов видят причину кибератак в широкой цифровизации бизнеса. Они полагают, что бизнес использует всё больше цифровых инструментов, каждый из которых может стать потенциальным источником опасности. При этом треть предпринимателей (35%) отмечают нехватку ресурсов на обеспечение защиты.

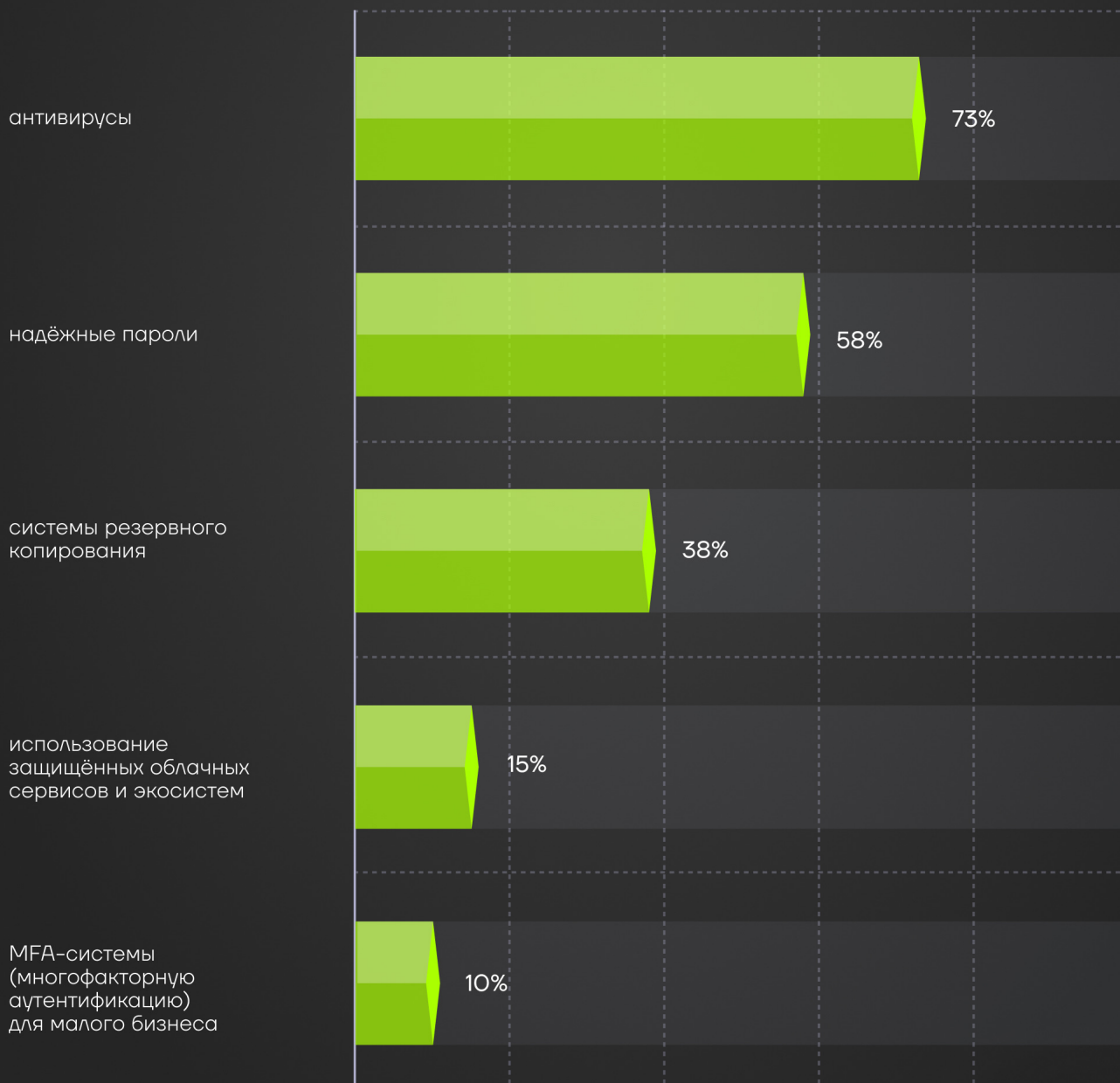
Какие главные причины распространения кибератак на малый и средний бизнес?



Меры безопасности: как победить мошенничество

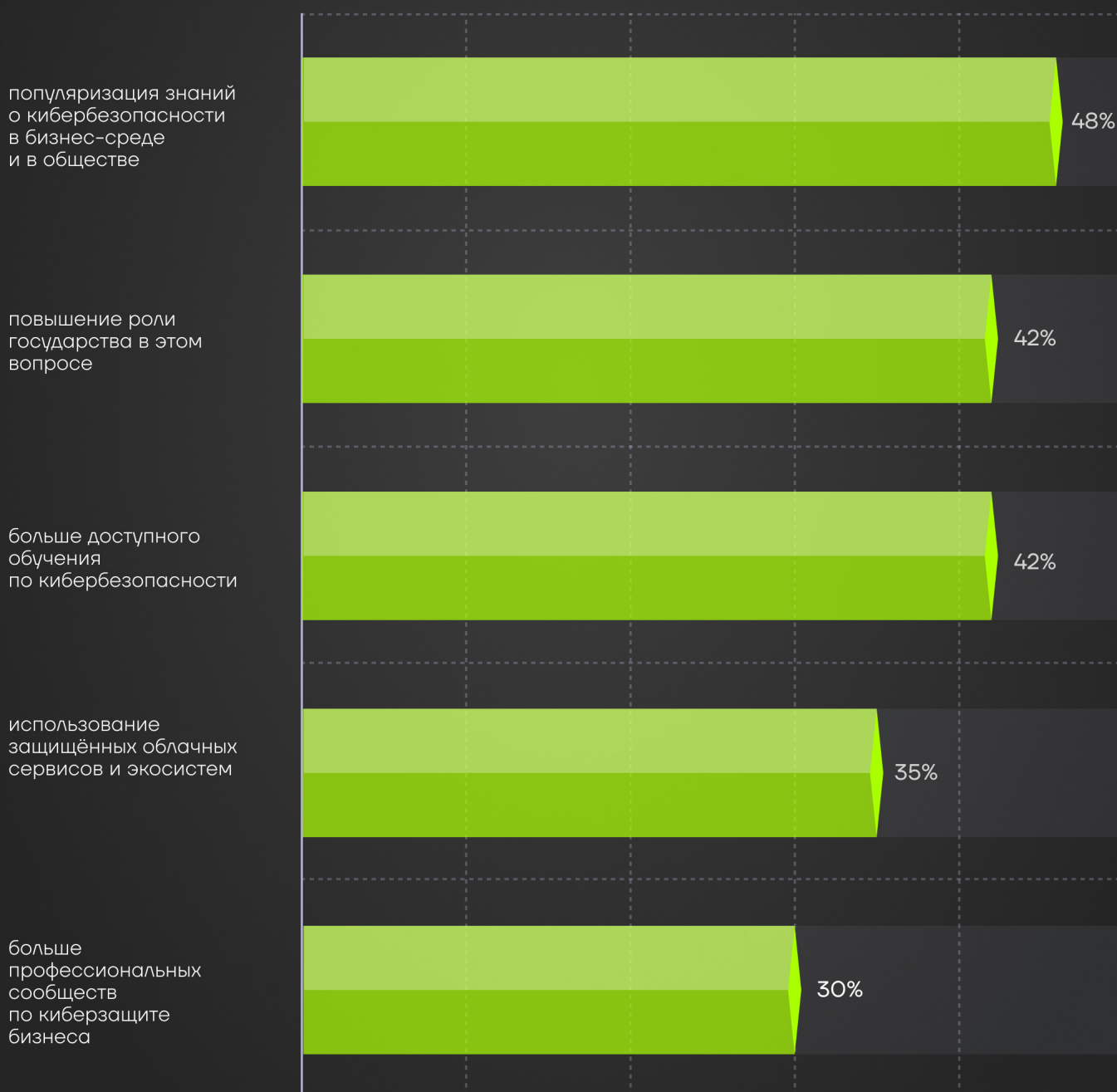
Среди наиболее распространённых средств защиты — антивирусы, они есть у 73% организаций МСП. Чтобы обезопасить бизнес-сервисы от несанкционированного входа, 58% предпринимателей следят за надёжностью используемых паролей, 10% применяют многофакторную аутентификацию. В 38% компаний внедрены системы резервного копирования данных, чтобы снизить риск их потери в случае атаки. А 15% используют защищённые облачные сервисы и экосистемы. Сервисы кибербезопасности по подписке рассматривают 33% участников опроса, а 15%, наоборот, не доверяют им и считают, что безопасность — задача штатных сотрудников. Ровно половина респондентов не определилась со своим отношением к покупке таких сервисов.

Какие меры предпринимает ваша компания для защиты от киберугроз?



Предприниматели понимают важность знаний по кибербезопасности. По мнению 48%, победить кибермошенничество поможет популяризация знаний по ИБ в бизнес-среде и обществе. Так, 35% предпринимателей хотят видеть больше профессиональных сообществ по киберзащите бизнеса, а 42% ждут более доступного обучения. При этом регулярное повышение квалификации сотрудников в области кибергигиены уже есть у 30% организаций МСП. Также опрошенные отметили важность мер со стороны государства: 42% выступают за повышение роли регулятора в борьбе с кибермошенниками.

Что нужно, чтобы победить или минимизировать кибератаки и кибермошенничество?





Для помощи малому и среднему бизнесу в рамках бизнес-клуба Кибердома работает проект CyberLink, где наши резиденты, эксперты в области кибербезопасности, помогают предпринимателям из других отраслей сделать чекап по цифровой гигиене и наметить шаги по внедрению простых, но эффективных решений для своего бизнеса. В клубе работает система менторства для предпринимателей, готовых сделать свой бизнес защищеннее и устойчивее



**руководитель бизнес-клуба
Кибердома**

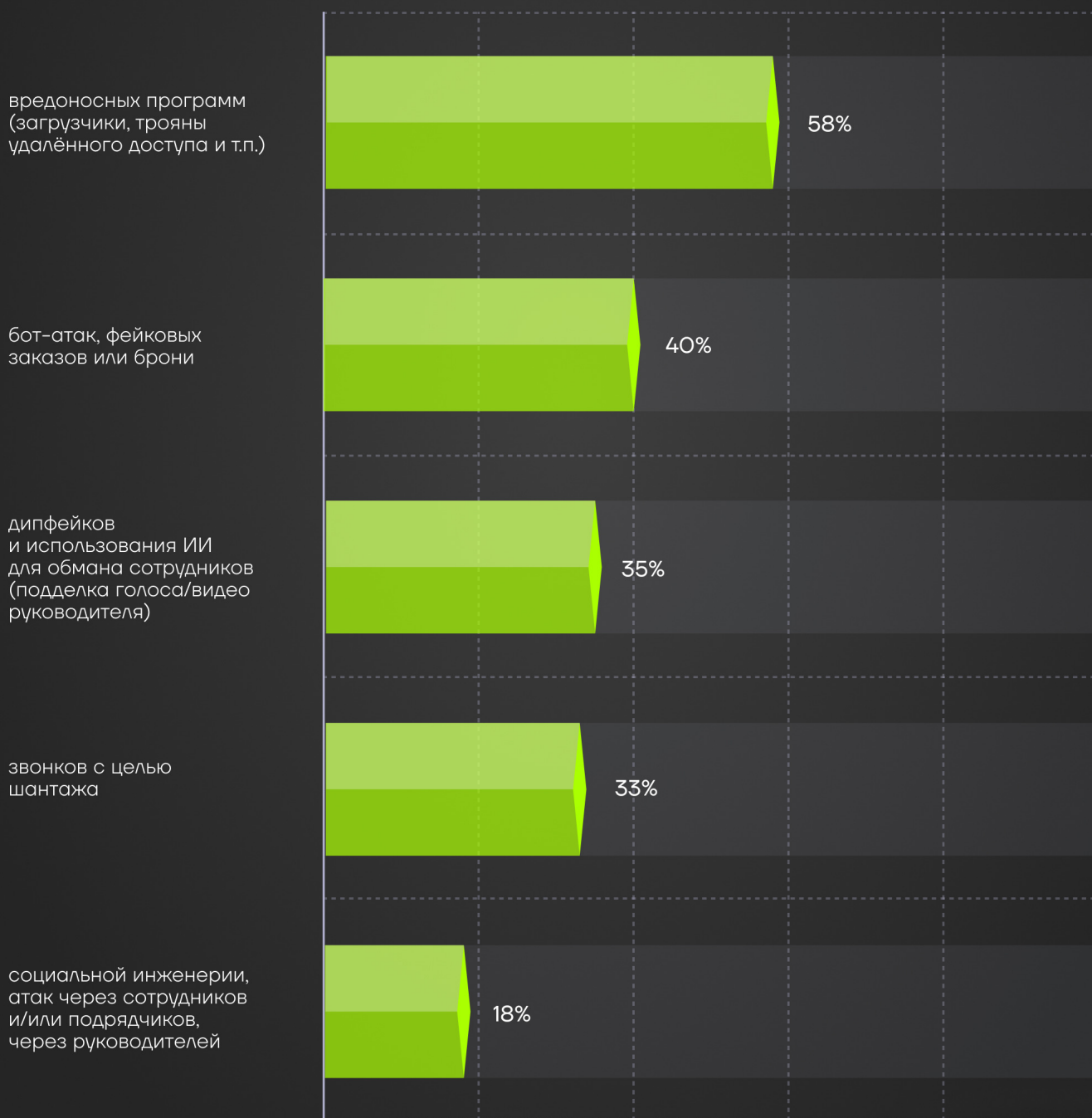
Ольга Орденова



Чего боится бизнес

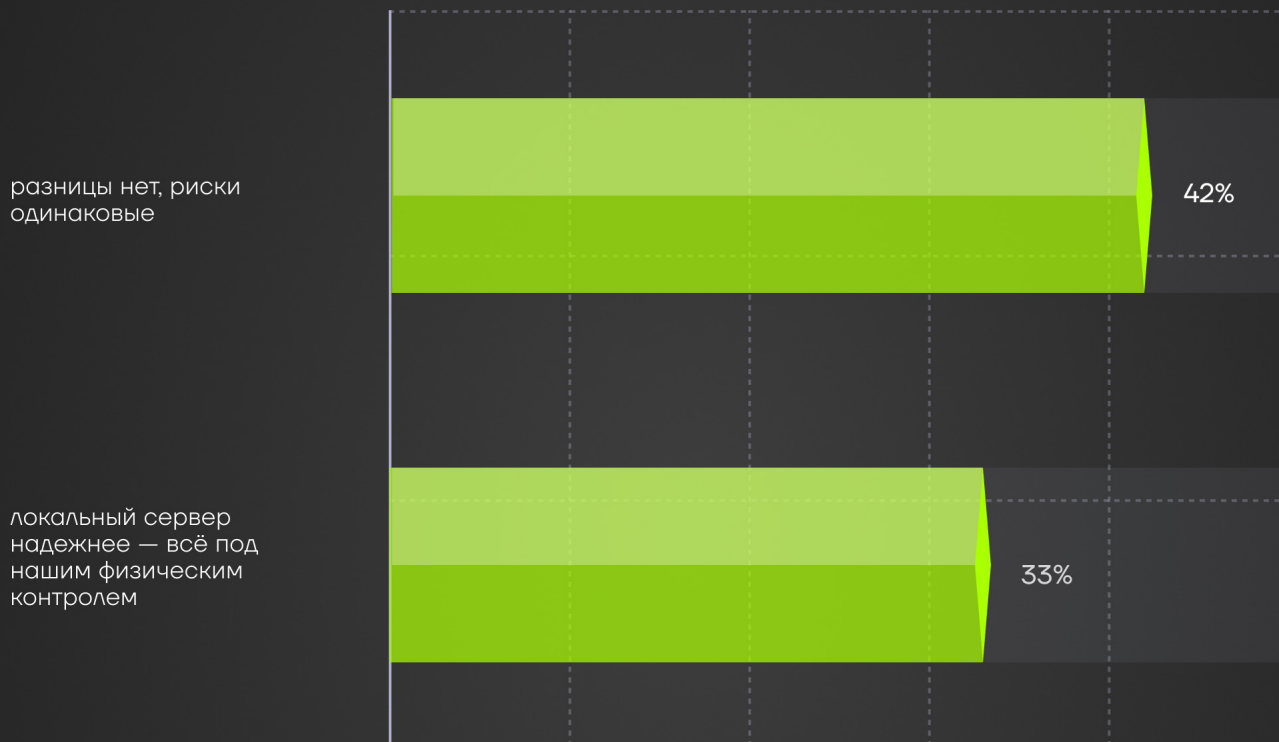
По мнению 58% участников опроса, самую большую опасность представляют вредоносные программы, 40% опасаются бот-атак. Мошенничества с использованием ИИ и дипфейков боятся 35% опрошенных, 33% — телефонного шантажа. Ещё 18% опасаются методов социальной инженерии, которые основаны на манипуляции людьми для получения чувствительной информации и выполнения действий, например, перевода денег или установки вредоносного ПО. Всё чаще эти методы применяются преступниками в цифровом пространстве.

Каких атак вы боитесь больше всего?



Более того, почти половина предпринимателей (48%) считает небезопасной облачную инфраструктуру и боится утечек из облака. Из-за этого треть опрошенных (33%) предпочитает размещать инфраструктуру на локальных серверах, так как она находится под контролем компании. Однако 42% респондентов не видят разницы между физической и облачной инфраструктурой.

Как вы оцениваете надёжность хранения данных в российском облаке по сравнению с локальными серверами (в офисе)?



О Кибердоме

Кибердом — проект, который объединяет кибербез-комьюнити, общество, бизнес и государство. Развивает культуру кибербезопасности в России, являясь её глобальным амбассадором на мировой арене. Проводит собственные мероприятия и развивает проекты для повышения киберграмотности бизнеса и общества. Гостями мероприятий в Кибердоме уже стали более 200 тыс. человек, а количество резидентов достигло 350 — представителей IT, ИБ, финтеха, e-commerce, ритейла и других

О Билайн бизнес

Билайн бизнес — один из крупнейших поставщиков телекоммуникационных и IT-сервисов в России. Специалисты Билайн бизнес развивают продукты и услуги, которые направлены на защиту от киберугроз и атак, продвигают технологии больших данных и аналитики, развивают решения в сфере «интернета вещей», голосовых сервисов с искусственным интеллектом, цифровой рекламы, цифровой трансформации бизнеса, а также облачную инфраструктуру и инструменты по защите и управлению ей