АГЕНТСТВО СТРАТЕГИЧЕСКИХ ИНИЦИАТИВ

SIDE

ИССЛЕДОВАНИЕ ЗАЩИЩЕННОСТИ ОТ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МАЛОГО И СРЕДНЕГО БИЗНЕСА

Январь 2024 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Высокие технологии, массовая цифровизация, ускоряющаяся в последние годы, особенно с началом пандемии COVID-19, перемещением жизни и работы в онлайн, кардинальным образом трансформируют социально-экономические процессы, оказывают влияние на все сферы жизни, в том числе на функционирование бизнеса и государства.

Вместе с цифровизацией набирают обороты и действия киберпреступников: получив новые технологические возможности и пользуясь недостаточным пониманием возможных угроз и нехваткой инструментов противодействия. Киберпреступления каждый год наносят ущерб на триллионы долларов по всему миру.

Существенное влияние на рост числа кибератак в России оказала геополитическая ситуация. Статистические данные различных источников существенно отличаются, но все они говорят, что в 2022–2023 гг. такие атаки увеличились в несколько раз[1].

Одним из ключевых изменений нового времени стал серьезный рост кибератак на малые и средней предприятия (МСП). Если еще в «доковидную» эпоху они довольно редко становились целью злоумышленников из-за низкой экономической целесообразности, а под ударом были крупный бизнес и объекты государственной критической инфраструктуры, то сейчас ситуация существенно изменилась.

Данное исследование подготовлено АНО «Агентство стратегических инициатив по продвижению новых проектов» совместно с ООО «Третья сторона» и является первой в России попыткой оценить защищенность субъектов малого и среднего предпринимательства, количество и последствия атак в условиях стремительного роста киберинцидентов в 2022–2023 гг., а также восприятие сферы информационной безопасности и типов угроз самим бизнесом.

Задача доклада — предложить информационно-аналитический материал для публичного обсуждения деловым сообществом, отраслью информационной безопасности, государством и другими участниками. Своевременное информирование и освоение бизнесом инструментов защиты позволят повысить эффективность управления киберрисками, снизить связанные с ними издержки и увеличить готовность к новым вызовам.

Доклад состоит из трех частей:

1. Киберугрозы нового времени
2. Опрос представителей МСП
3. Выводы и рекомендации

[1] Например, директор по развитию бизнеса сервисов кибербезопасности «Ростелеком-Солар» Алексей Павлов в интервью ТАСС назвал цифру в 9,6 раза (https://tass.ru/ekonomika/15562907 (дата обращения: 15.08.2022)).

ТЕРМИНОЛОГИЯ

CRM-системы — системы хранения и обработки данных клиентов.

SOC (Ситуационный операционный центр) — команда специалистов по информационной безопасности, обеспечивающая контроль и реагирование на инциденты в организации.

Антивирусное программное обеспечение (ПО) — специализированная программа, предназначенная для обнаружения вредоносного программного обеспечения и предотвращения нанесения ущерба от его работы.

Автоматическая система управления технологическим процессом (АСУТП) — программно-аппаратный комплекс, позволяющий управлять технологическим производством в полностью или частично автоматизированном режиме.

Информационная безопасность (ИБ), или кибербезопасность — комплекс мер, инструментов и процессов по сохранению и защите информации, компьютерных систем и информационной инфраструктуры от несанкционированного доступа, использования, изменения и уничтожения.

Кибератака — попытка получить несанкционированный доступ к информационной системе, либо вмешаться в ее работу.

МСП (малое и среднее предпринимательство) — организация или индивидуальный предприниматель с годовым оборотом до 2 млрд руб. и среднесписочной численностью персонала до 250 человек.

Угрозы информационной безопасности (или киберугрозы) — любое действие или событие, которое несет угрозу информационным системам, приводит к проникновению в них или их несанкционированному использованию.

Хакер (злоумышленник) — лицо, незаконно и умышленно проникающее в информационные системы либо влияющее на их работу с корыстной или иной целью.

Хактивизм (производное от понятий «хакер» и «активизм») — проведение кибератак без цели получения выгоды для продвижения политических или общественных идей.

ЧАСТЬ 1. КИБЕРУГРОЗЫ НОВОГО ВРЕМЕНИ

ВЛИЯНИЕ КИБЕРУГРОЗ НА ЭКОНОМИКУ И ОБЩЕСТВО

Кибериски затрагивают разные аспекты деятельности государства и жизни его граждан. Под угрозой находятся органы власти, транспорт, энергосистемы, больницы, образовательные учреждения, СМИ и многое другое.

Так, в 2022 г. результативная кибератака на систему управления железнодорожным движением в Дании привела к прекращению движения поездов по всей стране на сутки. В 2021 г. аналогичная ситуация возникла в Иране, а в 2022 г. в России была зафиксирована рекордная 30-часовая атака на инфраструктуру ОАО «РЖД». Примерно тогда же хакерам удалось атаковать «Яндекс.Такси» и отправить водителям фейковые заказы, что создало огромную пробку из машин такси.

В 2020 г. действия хакеров впервые привели к гибели пациента одной из больниц в Германии, когда отказ IT-систем привел к невозможности провести срочную операцию. В 2022 г. во Франции по такой же причине был приостановлен прием пациентов, многих из которых пришлось направить в другие лечебные учреждения.

В Израиле в марте 2022 г. крупная кибератака привела к тому, что недоступными стали сайты основных органов власти — пострадал даже сайт Моссада. Примерно тогда же хакерам удалось взломать сайты российских министерств и разместить там политические лозунги. Жертвами кибератак регулярно становятся сайты различных СМИ по всему миру от Ирана до США — как правило, речь идет о политическом хактивизме.

Компьютерные вирусы не раз использовались спецслужбами отдельных государств как оружие, применение которого привело к международным скандалам.

В случае с бизнесом речь идет уже о финансовом ущербе. Так, в мае 2017 г. вирусом-шифровальщиком WannaCry были заражены полмиллиона компьютеров в 150 странах мира. В том же году вирус Petya и его производные нанесли бизнесу и госорганам ущерб порядка 10 млрд долларов[2]. В создании обоих вирусов подозревают государственные агентства нескольких стран.

[2] https://www.researchgate.net/publication/324489505_What_PetyaNotPetya_Ransomware_Is_and_What_Its_Remidiations_Are (дата обращения: 21.10.2023)

Еще одной общественно значимой проблемой стали утечки персональных данных. По данным Group-IB в 2022 г. в сети оказалось порядка 1,3 трлн (!) строк данных[3], т.е. информация о каждом россиянине утекала в среднем около 10 раз. Общий объем утекших данных вырос за год в 40 (!) раз, в сети оказалась информация о примерно 100 млн российских граждан. Благодаря утечкам мошенники владеют качественной и регулярной обновляемой базой контактов большинства граждан нашей страны, что позволяет причинять больший ущерб. По данным Банка России, за 2022 г. россияне перевели мошенникам около 14 млрд руб[4].

Политический хактивизм и коммерческие атаки приводят к потере данных и наносят существенный прямой ущерб как государству, так и бизнесу. Если еще несколько лет назад «коммерческие» кибератаки были нацелены исключительно на получение выкупа от крупного бизнеса, то сейчас жертвами все чаще становятся органы власти и МСП.

В середине 2010-х гг. компания Group IB в рамках совместного исследования с ФРИИ и Microsoft оценила совокупный объем ущерба от кибератак в 0,25% ВВП России, или 203,3 млрд руб.[5], из которых около 123 млрд руб. составил прямой ущерб, а остальную сумму потратили на ликвидацию последствий. По оценке авторов доклада, в 2022 г. прямые потери от кибератак могли достичь 300 млрд руб. только прямого ущерба, что с учетом прочих расходов составило бы до 0,5% ВВП России.

С начала 2022 г. количество упоминаний киберинцидентов для бизнеса в СМИ выросло многократно, что отображает происходящие изменения.

ПОЗИЦИЯ ГОСУДАРСТВА

Слово «кибератака», привычное для специалистов по информационной безопасности, вошло в обиход предпринимателя и государственного служащего. Необходимость защиты от кибератак или хотя бы учета их возможности стала существенной частью государственной повестки.

Еще в 2013 г. Приказом Президента РФ от 15.01.2013 № 31с была создана ГосСОПКА — система предупреждения и ликвидации последствий кибератак. В 2015 г. аналогичный центр для банковского сектора появился в Центральном банке России. Обе системы ориентированы в первую очередь на крупный бизнес, создавшие собственные SOC-центры — способ централизованного реагирования на инциденты в сфере ИБ.

После событий 2022 г. Россия взяла курс на ускоренное импортозамещение, в том числе в области ИБ-продуктов. Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» фактически запретил использование иностранного ПО для критической инфраструктуры, а Указом Президента РФ от 01.05.2022 № 250 государственным органам был установлен запрет на использование средств защиты из недружественных стран.

Вопрос информационной безопасности активно входит в поле внимания властей на федеральном уровне. Так, Правительство РФ утвердило Распоряжение от 22.12.2022 № 4088-р «О Концепции формирования и развития культуры информационной безопасности граждан Российской Федерации».

Ключевые пункты Концепции, актуальные для данного исследования:

- консолидация усилий органов государственной власти, неправительственных и коммерческих организаций в работе по повышению грамотности граждан Российской Федерации в вопросах информационной безопасности;
- проведение адаптированной к разным категориям граждан Российской Федерации информационной кампании как основного способа повышения культуры информационной безопасности и др.

[3] https://www.facct.ru/media-center/press-releases/database-2022/ (пресс-релиз на официальном сайте компании (дата обращения: 21.10.2023))
[4] https://www.cbr.ru/analytics/ib/operations_survey_2022/ (аналитический отчет на сайте ЦБ (дата обращения: 21.10.2023)
[5] https://www.iidf.ru/media/articles/trends/kiberprestupnost-v-rossii-ugrozy-masshtaby-sredstva-borby/ (пресс-релиз на сайте ФРИИ, одного из участников исследования (дата обращения: 21.10.2023)

КИБЕРБЕЗОПАСНОСТЬ В РОССИИ В 2022–2023 ГГ.

В 2022 г. количество инцидентов в сфере ИБ по данным Positive Technologies выросло на 20,8%[6]. По данным «Ростелеком-Солар», основной целью злоумышленников стали государственные структуры: количество атак увеличилось в 7 раз. В то же время, Group-IB оценивает рост числа финансово-мотивированных атак на российский бизнес на уровне 300%. Почти половина компаний сегмента МСП столкнулась с кибератаками, при том, что до 2022 г. для злоумышленников они не представляли интереса.

Данные факторы подталкивают к росту рынок услуг ИБ. Согласно опубликованному в июле 2023 г. исследованию Фонда «Центр стратегических разработок»[7], объем рынка ИБ по итогам 2021 г. составил 186,9 млрд руб. в деньгах заказчика, а по итогам 2022 г. — 193,3 млрд руб. Ожидается, что к 2026 г. объем рынка достигнет 470 млрд руб., фактический рост в 2,5 раза. Доля услуг на рынке составляет порядка 25–27% от всего объема. При этом значительную часть услуг (64%) в 2022 г. составили внедрение, проектирование и сопровождение — обеспечение жизненного цикла средств защиты. Еще порядка 25% — это консалтинг и оценка защищенности, 6% — аутсорсинг и 5% — расследование инцидентов.

Можно выделить две ключевые причины роста рынка: изменение геополитической обстановки, приведшее к уходу западных вендоров, и многократный рост числа кибератак в России.

Наиболее точно российский рынок кибербезопасности можно охарактеризовать как «крупный бизнес для крупного бизнеса». Например, топ-7 компаний-вендоров средств защиты сейчас занимают половину (!) всего рынка, а с учетом ухода западных игроков (4 из 10 крупнейших вендоров средств защиты) их доля существенно вырастет.

Еще одной особенностью рынка ИБ услуг являются цепочки субподрядов: нередко компании-подрядчики «продают» заказы своих клиентов конкурентам. Это приводит к ощутимому завышению стоимости услуг: периодически можно наблюдать до пяти фактов перепродаж. При этом конечный исполнитель часто получает небольшую сумму от заказа, а на рынке появляются компании, в штате которых специалистов по продажам больше, чем специалистов по информационной безопасности.

Одной из причин сложившейся ситуации является нехватка специалистов ИБ: так, по словам заместителя Председателя Правления «Сбера» Станислава Кузнецова, в России не хватает «десятков тысяч специалистов»[8]. В госорганизациях ситуация еще сложнее: Президент «Академии криптографии» Александр Шойтов называл цифру в 80% компаний и организаций, заявивших о дефиците необходимых кадров[9], при этом быстро восполнить дефицит компетентных специалистов невозможно. Всего в России, по разным оценкам, не хватает от 50 до 100 тыс. ИБ-специалистов.

Еще несколько лет назад действия хакеров наносили ущерб в первую очередь крупным компаниям. Сейчас угрозе подвергаются бизнесы любого размера.

ПОЧЕМУ МСП ВЫНУЖДЕНЫ ДУМАТЬ О КИБЕРБЕЗОПАСНОСТИ

Согласно докладу компании Accenture[10], уже около 43% атак по всему миру нацелены на малый и средний бизнес и только 14% этих предприятий готовы защищать данные.

Долгое время стратегия «игнорирования угрозы» была позволительна для МСП и в России, и в мире, так как небольшие компании взламывались достаточно редко, атаки не были экономически привлекательными для киберпреступников. В России до 2022 г. многие компании становились случайными жертвами шифровальщиков — программ-вымогателей, создатели которых требовали деньги за восстановление зашифрованной информации.

---

[6] Доклад «Актуальные киберугрозы: итоги 2022 года», https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/(дата обращения: 21.10.2023)
[7] «Прогноз развития рынка кибербезопасности в Российской Федерации на 2023-2027 годы», https://www.csr.ru/upload/iblock/0da/cl25xkzy12if5l4xs425yi25ezp1a11z.pdf(дата обращения: 21.10.2023)
[8] https://www.rbc.ru/rbcfreenews/63169d139a79477c5dfbdee6) (дата обращения: 21.10.2023)
[9] https://rg.ru/2023/03/12/mehanizm-bagbaunti-i-ataka-za-voznagrazhdenie-kak-reshit-problemu-deficita-specialistov-po-kiberbezopasnosti.html(дата обращения: 21.10.2023)
[10] Accenture Cost of Cybercrime Study, https://www.getastra.com/blog/security-audit/small-business-cyber-attack-statistics(дата обращения: 21.10.2023)

Главные причины, по которым российские МСП все еще игнорируют ИБ-угрозы, — высокая стоимость услуг и ориентированность отрасли на крупнейшие компании, особенно на банки и других игроков финансового сектора. Работать с такими клиентами проще, прибыльнее, они традиционно тратят значительные деньги на защиту, часто покупают множество как продуктов, так и услуг.

Расходы на ИБ малого и среднего бизнеса в мире, по оценке «Лаборатории Касперского», оказались в среднем на довольно высоком уровне 38 тыс. долларов в год (3 млн руб. по курсу на начало 2023 г.)[11]. С бюджетами на ИБ в России ситуация кардинально иная, и зачастую расходы находятся на минимальном уровне. В связи с этим на рынке не так много продуктовых решений, ориентированных на МСП.

При этом стоимость только одной проверки защищенности инфраструктуры (пентеста) в большинстве случаев составляет 1–2 млн руб. И МСП зачастую были вынуждены ограничиваться только самым необходимым — покупкой антивирусных программ и базовыми настройками безопасности.

Проблему дороговизны услуг можно назвать общемировой — на Западе крупный бизнес не раз платил десятки миллионов долларов за восстановление данных и тратил сопоставимые суммы на защиту, а МСП нередко несли ущерб в сотни тысяч долларов. В 2021 г. российские МСП в среднем платили 3 млн руб. за расшифровку данных[12], но сопоставимый бюджет на ИБ есть далеко не у всех компаний.

Еще одна причина — слабая информированность сегмента МСП о возможных угрозах и способах защиты от них. Отсутствие необходимости защищаться от множества реальных киберугроз и внезапное изменение ландшафта угроз в 2022 г. поставили МСП в уязвимое положение.

Ввиду отсутствия явных и значимых угроз долгое время внутри МСП не вырабатывались соответствующие компетенции. Собственники бизнеса и менеджмент не привыкли инвестировать в информационную защиту. Вследствие отсутствия ИБ-компетенций зачастую даже при наличии бюджета на безопасность МСП не имеют возможности грамотно им распорядиться.

Между тем с каждым годом массовая цифровизация увеличивает долю компаний, которые создают, хранят и передают данные о деятельности своего бизнеса, клиентах, партнерах. За последние два года картина для сегмента МСП перевернулась, а российский ландшафт информационной безопасности буквально разделился на «до» и «после». Личные кабинеты предпринимателей и клиентов, собственный софт, платежные данные или CRM-система — все, что видно в сети Интернет, уязвимо. В геополитических и технологических условиях жертвой преступников может стать любая компания, и вопрос только в величине понесенных потерь.

Киберугрозы и последствия атак все сильнее зависят от отраслевой принадлежности бизнеса.

Для технологических, производственных компаний или сектора логистики уровень угрозы и потенциальных потерь от атак гораздо выше, чем, например, для представителей сектора услуг. Причина понятна: стоимость простоя оборудования, восстановления работы парка станков или остановки грузоперевозок на несколько суток может быть критически высокой для любого бизнеса. Кроме того, мошенники активно атакуют небольшие торговые онлайн-площадки, чтобы добраться до их клиентов, а мобильные приложения — ради доступа к платежной информации.

При этом для некоторых отраслей даже сейчас стратегия «игнорирования угроз» по-прежнему является приоритетной в управленческих действиях. Например, для индустрий общественного питания или сферы услуг в худшем случае, они временно потеряют контроль над сайтом или системой бронирования заказов из-за взлома программного обеспечения. Но сотни и тысячи обманутых клиентов могут отказаться от таких услуг. Пока об объеме ущерба в данных сферах чаще начинают задумываться только при повторяющихся кибератаках.

При этом необходимо понимать, чем более автоматизирован и технологичен бизнес, тем сильнее зависит от работы с данными, реальнее угроза информационной безопасности.

[11] https://www.kaspersky.ru/about/press-releases/2023_v-sleduyushie-tri-goda-rossijskie-kompanii-planiruyut-uvelichit-byudzhet-na-kiberbezopasnost-na-14 (дата обращения: 21.10.2023)
[12] https://www.facct.ru/media-center/press-releases/bell-club/ (пресс-релиз на сайте исследователя (дата обращения: 21.10.2023))

УГРОЗЫ ПО ТИПАМ АТАК

В современных российских реалиях эксперты выделяют три основных типа угроз для МСП.

1. Шифровальщики и программы-вымогатели.

Три года назад компания CISCO именно шифровальщиков назвала одной из главных цифровых угроз для бизнеса. Их создатели, как правило, имеют финансовую мотивацию — зашифровать данные и получить за них выкуп. Для МСП они опасны из-за возможной потери данных и остановки технологических процессов, тем более что в отличие от крупных организаций резервное копирование в МСП настроено ощутимо хуже или отсутствует. После 2022 г. количество атак с использованием шифровальщиков на МСП выросло в 5 раз[13].

2. Действия активистов и недовольных сотрудников.

Основная цель — нанесение максимального ущерба. Для таких людей и организаций финансовая мотивация уходит на второй план, они выбирают жертв по принадлежности к отдельной стране, индустрии или просто атакуют бывшего работодателя.

Самым ярким примером «финансово немотивированной» атаки можно назвать взлом МосгорБТИ — государственного предприятия, которое занимается сбором и обработкой технической информации о московской недвижимости. Эта организация хранит сведения об истории перепланировок в московских квартирах. Так, получение выкупа даже в случае исключительно успешной атаки было невозможным, злоумышленники это понимали, но их это не останавливало. Точно такая же ситуация сложилась с МСП, атаковать которых для злоумышленников раньше было неразумно из-за малой стоимости выкупа. Сейчас их цель — не прибыль, а максимальный ущерб.

С подобными ситуациями регулярно сталкиваются и небольшие коммерческие компании: злоумышленники требуют от них выкуп, который может быть сопоставим с годовым оборотом компании. В некоторых случаях невозможность восстановления зашифрованных данных приводила к банкротству бизнеса.

3. Мошенничество.

Оно особенно актуально для маркетплейсов и компаний, занимающихся электронной коммерцией. Мошенники нередко получают доступ к базе клиентов и начинают звонить от имени компании, предлагая «уникальные условия» и «огромные скидки». В худшем случае они действуют заодно с действующими сотрудниками — вспоминаем историю Wildberries, когда злоумышленники продавали рекламу на продвижение товаров, имея доступ к внутренним инструментам.

Даже не имея компетенций в ИБ, бизнесу важно быть «квалифицированным заказчиком», в противном случае он имеет огромный шанс получить набор дорогих и малополезных продуктов и услуг.

[13] https://www.kommersant.ru/doc/5843753

ПОСЛЕДСТВИЯ ДЛЯ МСП

Киберугрозы порождают множество совершенно разных рисков для бизнеса — это прямой финансовый ущерб, репутационные потери, издержки и штрафы.

Прямые финансовые потери.

По данным «Лаборатории Касперского», средний ущерб от кибератак для МСП составил порядка 32 000 долларов, причем с высокой вероятностью эта цифра в реальности несколько меньше, а общее количество успешных атак со сравнительно небольшим ущербом — больше[14]. Успешные атаки наносят прямой ущерб бизнесу, препятствуют его нормальному функционированию и создают дополнительные затраты как на восстановление данных и инфраструктуры, так и на организацию функции информационной безопасности, включая покупку лицензий на ПО, дополнительные расходы на заработные платы и услуги сторонних подрядчиков по ИБ.

В соответствии с КоАП юрлицо могут оштрафовать на сумму до 300 000 руб. по ст. 13.11 о нарушении правил о персональных данных в случае их повторных утечек.

В настоящее время в России используется практика минимальных либо отсутствующих штрафов за утечку персональных данных, но внимание государства к этому вопросу в скором времени может привести к ужесточению законодательства и правоприменительной практики.

Репутационные потери.

Клиенты компании, которая по собственной халатности допустила утечку персональных данных, будут менее лояльными к ней. В случае если в сети окажется критическая клиентская информация, способность такой компании эффективно вести бизнес окажется под угрозой. Репутационные потери приводят к сокращению количества клиентов.

Особо следует отметить угрозу использования злоумышленниками зараженной компьютерной инфраструктуры жертвы для проведения дальнейших атак. В 2023 году имели место несколько примеров использования инфраструктуры отдельных предприятий МСП для распространения вредоносного ПО, о котором владельцы систем узнавали только после визита правоохранительных органов. Применение МСП злоумышленниками «втемную» может привести не только к очевидным юридическим последствиям, но и к изъятию оборудования в случае, если таковое использовалось для атаки на критическую инфраструктуру страны. Как правило, распространение вредоносного ПО в этой ситуации идет в автоматическом режиме, но для МСП этот факт особого значения не имеет.

МСП в России сталкиваются с недостаточностью понимания проблем киберугроз, а также опыта и компетенций по защите бизнеса. Необходимо повышать осведомленность предпринимателей, создавать условия для подготовки специалистов ИБ, обеспечить доступ к качественным и недорогим инструментам и технологиям.

В России сформировался замкнутый круг — представители малого и среднего бизнеса зачастую не понимают, как им строить ИБ, количество кибератак с каждым годом растет, а специалистов по ИБ катастрофически не хватает. В итоге именно небольшие компании, особенно располагающие IT-инфраструктурой, но не имеющие возможностей для эффективной защиты, оказываются в зоне риска.

[14] Сохраненная копия пресс-релиза:
https://www.kaspersky.ru/about/press-releases/2021_vizhu-cel-samyj-bolshoj-usherb-ot-kiberincidentov-v-2021-godu-dlya-rossijskogo-biznesa-byl-svyazan-s-targetirovannymi-atakami,(дата обращения 12.10.21)

ЧАСТЬ 2. ОПРОС ПРЕДСТАВИТЕЛЕЙ МСП

ОБЩАЯ ИНФОРМАЦИЯ ОБ ОПРОСЕ

Опрос проводился в III-IV кварталах 2023 г. с целью оценки ситуации в сфере ИБ предприятий малого и среднего бизнеса. Исследование проводилось с участием 701 респондента, удаленно, анонимно, путем анкетирования.

Были размещены ссылки на анкеты на порталах региональных органов власти и общественных организаций, а также целевой рассылки участникам данных организаций.

Методологическое уточнение:

В ходе анализа полученных данных в большей части ответов респондентов была выявлена их зависимость от размера годовой выручки компании, поэтому в качестве границы категории мы использовали разделение:

- в категорию «малые МСП» вошли организации с годовой выручкой до 400 млн руб., т.е. микропредприятия и часть малых предприятий;
- в категорию «крупные МСП» — предприятия с годовой выручкой от 400 млн до 2 млрд руб., т.е. часть малых и средние компании.

Использование данного разделения оставляет в выборке зрелые предприятия, близкие к среднему бизнесу и позволяет получить большее количество наблюдений.

КЛЮЧЕВЫЕ ВЫВОДЫ И РЕЗУЛЬТАТЫ ОПРОСА

Поведение МСП в части кибербезопасности реактивно. Бизнес начинает заниматься ИБ после того, как сталкивается с кибератаками и иными ИБ-инцидентами.

Ключевым выводом опроса является факт начала активных кибератак на сегмент МСП, что в целом соответствует мировым трендам, описанным в части 1 доклада. **Так, почти 45% всех опрошенных компаний сообщили о наличии инцидентов в сфере ИБ за прошедший год, при этом порядка 30% из имевших такие инциденты оценивают понесенный ущерб как умеренный или критический.**

Порядка 40% опрошенных компаний за прошедший год не понесли расходов на ИБ вообще. Мы предполагаем, что реальная картина может быть несколько иной, так как часть компаний покупает «коробочкое» антивирусное ПО (порядка 40% опрошенных), расходы на которое заложены в ИТ или административные бюджеты. **Всего 4% компаний имеют полноценное бюджетирование.** Значительная часть МСП оценивает свои расходы на ИБ как нулевые — МСП либо игнорируют угрозы в сфере ИБ, либо не могут себе позволить эффективные средства защиты.

Среди понесших ущерб от кибератак компаний доля имевших расходы на ИБ за прошедший год выше, чем среди не понесших ущерб. **Мы предполагаем, что это связано с необходимостью восстановления инфраструктуры и построения защиты уже после произошедшего инцидента, а не до него.**

Расходы на ИБ ожидаемо растут вместе с выручкой — в случае среднего бизнеса (оборот до 2 млрд рублей в год) почти 40% участников опроса заказывали ИБ-услуги у сторонних компаний, а каждый десятый занимался полноценным бюджетированием ИБ.

При этом «крупные МСП» подходят к управлению рисками информационной безопасности более серьезно: **порядка 75% компаний этого сегмента имеют расходы на ИБ, а сами компании практикуют системное бюджетирование и внедрение ИБ в 4 раза чаще**, чем в среднем по выборке опроса.

Также в **70% случаев у компаний данной категории в штате есть специалист, ответственный за ИБ,** что приблизительно в 2 раза чаще, чем у компаний с выручкой до 400 млн рублей. «Крупные МСП» вынуждены нанимать людей, конкурируя с крупным бизнесом и государственными структурами на рынке труда в условиях дефицита компетентных специалистов.

С ростом выручки компании чаще обеспокоены уязвимостью систем автоматизации. Так, «малые МСП» в 40% случаев ключевой считают угрозу своему сайту. «Крупные МСП» в 37% случаев видят ключевую угрозу своим АСУТП (автоматические системы управления техпроцессом).

Для многих МСП актуальной является возможность получения поддержки государства для приобретения ИБ-продуктов. При этом у МСП остается сильный запрос на нефинансовую помощь: свыше 40% как «крупных», так и «малых МСП» заявили об актуальности для них программ по информированию о существующих рисках. **Информация об ИБ-угрозах для МСП так же актуальна, как и прямая финансовая поддержка.**

Что касается отдельных отраслей, **мы не выявили значительной разницы между ними как с точки зрения поведения, так и с точки зрения понесенного ущерба.**

ОБЩАЯ ИНФОРМАЦИЯ ПО ВЫБОРКЕ

Региональная представленность. В опросе принял участие 701 представитель субъектов МСП из 63 регионов России.

Топ-5 регионов по месту регистрации участников опроса

Название региона	Доля анкет (%)
Республика Татарстан (Татарстан)	24,0
Московская область	15,8
Астраханская область	7,3
Ростовская область	5,0
Кабардино-Балкарская Республика	4,4

Отраслевая представленность. Для выбора отрасли было предложено 26 вариантов и возможность указать свой вариант. Наибольшую представленность в выборке респондентов составили компании розничной торговли и производства товаров. Топ —5 отраслей составили 57% в общей выборки.

Топ-5 отраслей участников опроса

Отрасль	Доля анкет (%)
Розничная торговля	15,8
Производство товаров	11,1
ЖКХ	10,7
Услуги для бизнеса	10,1
IT, системная интеграция, разработка ПО, IT-консалтинг	9,3

Представленность по годовой выручке. Наиболее частыми респондентами в нашей выборке становились компании с выручкой до 120 млн рублей в год — микропредприятия.

Доля микропредприятий в выборке опроса ниже, чем в среднем по МСП (81,9% против 96,2%), а малого и среднего бизнеса — существенно выше, чем в среднем по стране: 18,2% против 4%, что позволяет лучше проанализировать проблемы сравнительно малочисленных малых и средних предприятий («крупного МСП»).

Распределение участников опроса по годовой выручке

Годовая выручка	Доля анкет (%)	Всего в России, %[15]
До 60 млн руб.	70,2	96,2 (микропредприятия)
До 120 млн руб.	11,7	
До 400 млн руб.	9,6	3,5 (малые предприятия)
До 800 млн руб.	3,3	
До 2 млрд руб.	5,3	0,3 (среднее предприятие)

[15] https://www.researchgate.net/publication/324489505_What_PetyaNotPetya_Ransomware_Is_and_What_Its_Remidiations_Are (дата обращения: 21.10.2023)

ИНЦИДЕНТЫ В СФЕРЕ БЕЗОПАСНОСТИ И УЩЕРБ

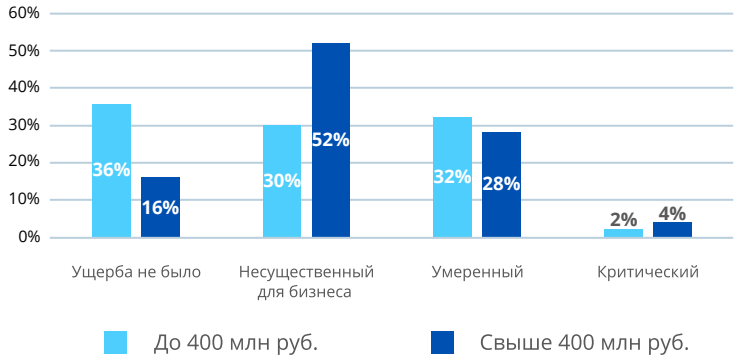
В данном блоке вопросов мы хотели узнать, как сами представители МСП оценивают ущерб от инцидентов в сфере ИБ за последний год и его влияние на их бизнес. Кроме того, мы хотели получить более детальную информацию о типе инцидентов и его последствиях.

Как было указано выше, порядка 45% опрошенных компаний сталкивались с инцидентами в сфере ИБ либо кибератаками за прошедший год.

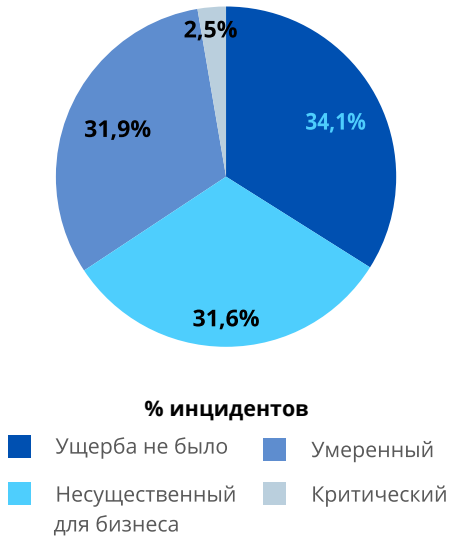
Тот факт, что сравнительно малое количество респондентов сообщило о критическом ущербе их бизнесу, может быть связан с тем, что они могли прекратить свое существование вследствие кибератаки.

Приблизительно 30% из компаний, столкнувшихся с ИБ-инцидентами, оценивает его как умеренный или критический.

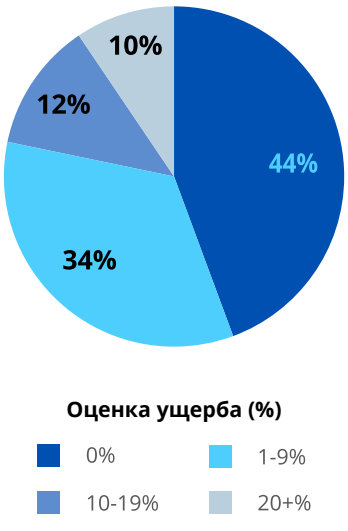
ИНЦИДЕНТЫ В СФЕРЕ БЕЗОПАСНОСТИ «МАЛЫХ» И «КРУПНЫХ» МСП



РАСПРЕДЕЛЕНИЕ УЩЕРБА ОТ ИНЦИДЕНТОВ В СФЕРЕ БЕЗОПАСНОСТИ



ВЕЛИЧИНА УЩЕРБА К ОБОРОТУ КОМПАНИИ



ПРОИСХОЖДЕНИЕ ИБ-ИНЦИДЕНТА

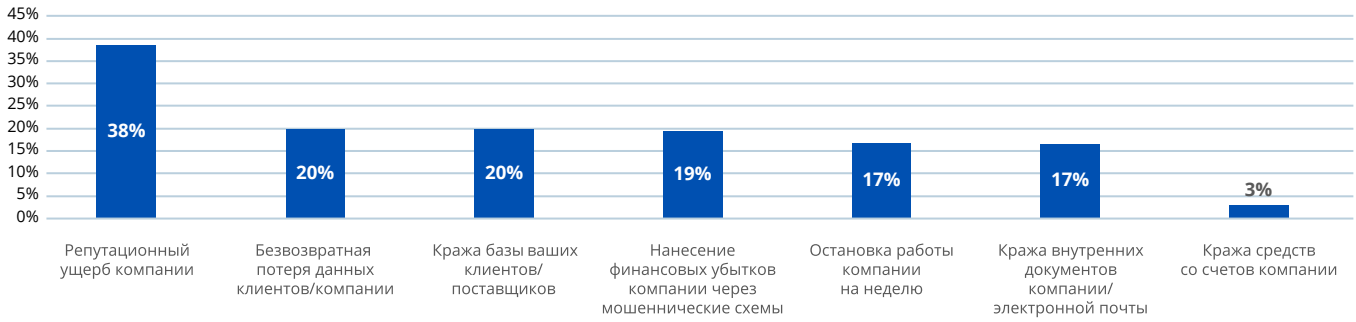
Порядка 70% респондентов на вопрос «Оцените ущерб от связанных с ИБ инцидентов от оборота компании» не ответили и можно предположить, что многие МСП либо не могут дать точную оценку, либо не хотят говорить о потерях. Среди ответивших (т.е. понесших ущерб) большинство оценило его как нулевой.

В приблизительно 70% случаев инциденты в сфере ИБ имели исключительно внешнюю или смешанную природу.

Для МСП актуальна комплексная и доступная защита от всего спектра возможных киберугроз.

Чаще всего опрошенные МСП несли в результате киберинцидентов репутационный ущерб — 38%, реже всего (в 3% случаев) — кража средств со счетов.

ВИДЫ УЩЕРБА, ПОНЕСЕННОГО МСП ОТ КИБЕРАТАК

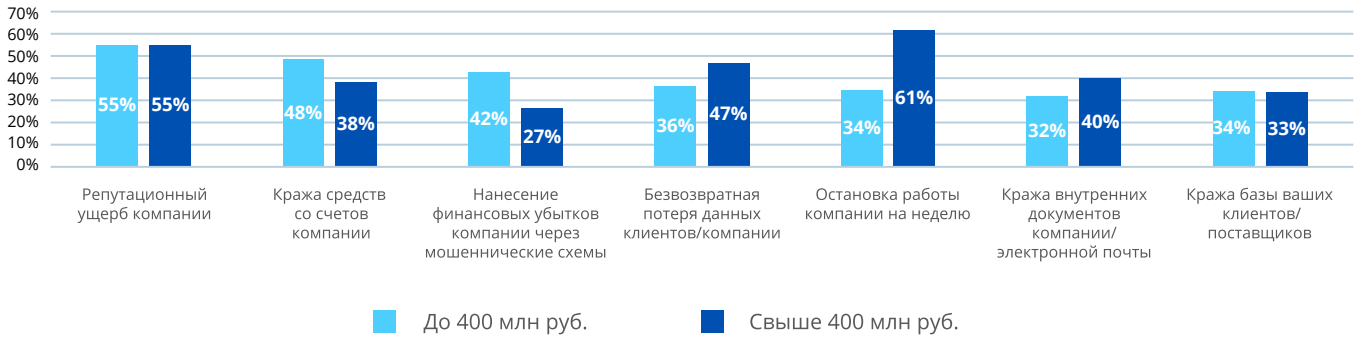


ЧЕГО БОЯТСЯ МСП?

Как показали результаты опроса, самооценка ключевых угроз для бизнеса зависит от уровня автоматизации, размера и сферы деятельности компании. Ожидаемо, для МСП с большей выручкой более опасна приостановка бизнес-процессов ввиду того, что их восстановление занимает длительный срок, а сами они опираются на технологически сложные системы. В то же время для микропредприятий данная проблема менее актуальна — они чаще боятся кражи средств и потери доступа к сайту / базе клиентов.

В данном блоке вопросов мы хотели узнать, чего представители МСП больше всего боятся и что считают наиболее уязвимым.

КЛЮЧЕВЫЕ УГРОЗЫ ДЛЯ БИЗНЕСА



В 55% случаев МСП боятся нанесения репутационного ущерба как наибольшей угрозы бизнесу, реже всего (в 33% случаев) — кражи внутренних документов. Для МСП, существующих в высококонкурентной среде, потеря репутации и клиентов, зачастую может нанести большой урон. Внутренняя документация менее важна, так как в ней не содержится особо конфиденциальная информация.

«Малые МСП» чаще опасаются мошеннических схем и кражи средств со счетов, т. е. факторов, в большей степени угрожающих собственникам-физлицам.

«Крупные МСП» видят для себя угрозой приостановку бизнес-процессов, что обусловлено стоимостью их восстановления.

Угрозу кражи средств со счетов компании МСП склонны переоценивать: свыше 40% опрошенных оценили ее как значимую, но только 3% произошедших инцидентов были связаны с такого рода событиями.

КЛЮЧЕВЫЕ ТОЧКИ УЯЗВИМОСТИ МСП

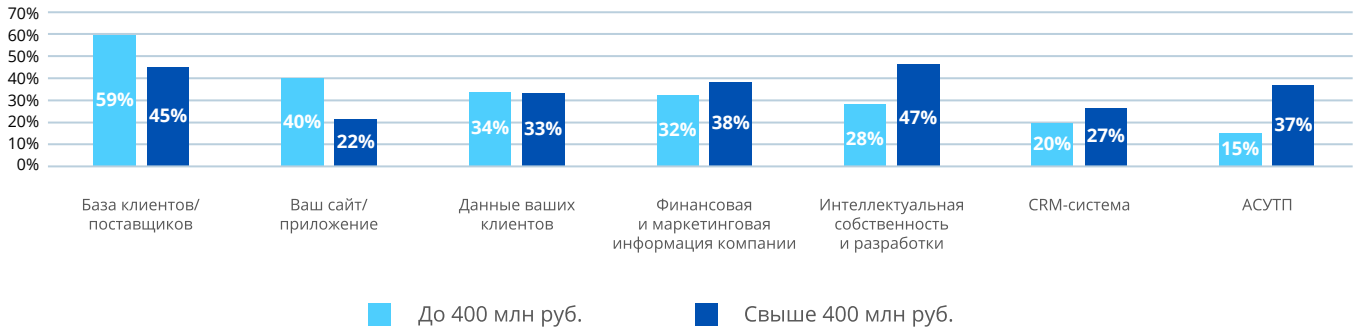
Наиболее важными для себя представители МСП называли **базы клиентов или поставщиков (58,2% опрошенных), а также собственный сайт или приложение (38,4% опрошенных).** Реже всего — CRM-системы и АСУТП (автоматические системы управления техпроцессом) — их наиболее важными посчитали только 17,1% ответивших. Такие ответы закономерны: для большинства небольших компаний автоматизация бизнеса менее важна.

Наличие систем автоматизации является прямым следствием увеличения масштаба бизнеса и становится дополнительным источником ИБ-рисков.

Более трети всех «крупных МСП» указали ее как важный актив. Крупные предприятия чаще занимаются инновационной деятельностью и воспринимают кражу интеллектуальной собственности как серьезную угрозу.

Для ряда микропредприятий системы автоматизации (АСУТП) имеют определенную ценность: мы предполагаем, что за них могли принять CRM-систему или иной способ управления клиентами. Роль АСУТП и CRM-систем очень существенно растет с увеличением масштаба бизнеса.

КЛЮЧЕВЫЕ ТОЧКИ УЯЗВИМОСТИ МСП

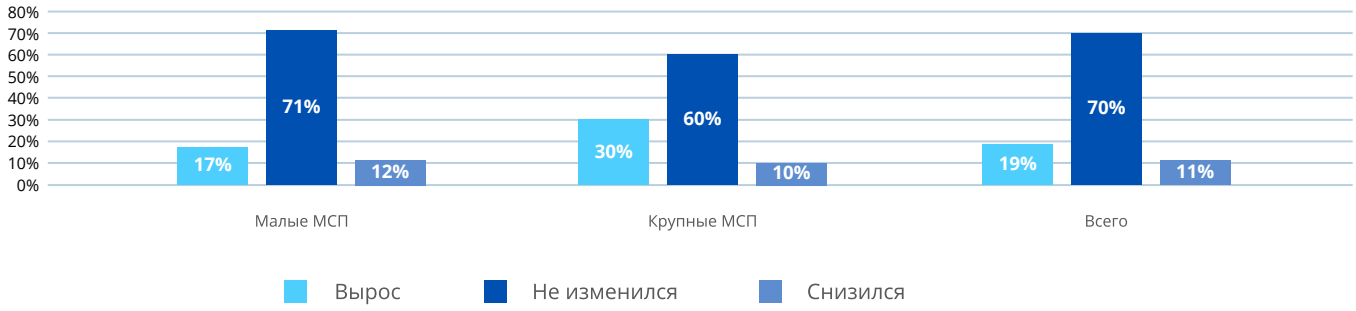


САМООЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ

В данном блоке вопросов мы хотели узнать, как сами МСП оценивают изменение своего собственного уровня защищенности.

70% респондентов считают, что их уровень защищенности от киберугроз за последний год не изменился. Крупные МСП чаще говорят о том, что их уровень защищенности вырос, что может быть связано с более глубоким пониманием угрозы и большим объемом расходов на ИБ.

САМООЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ

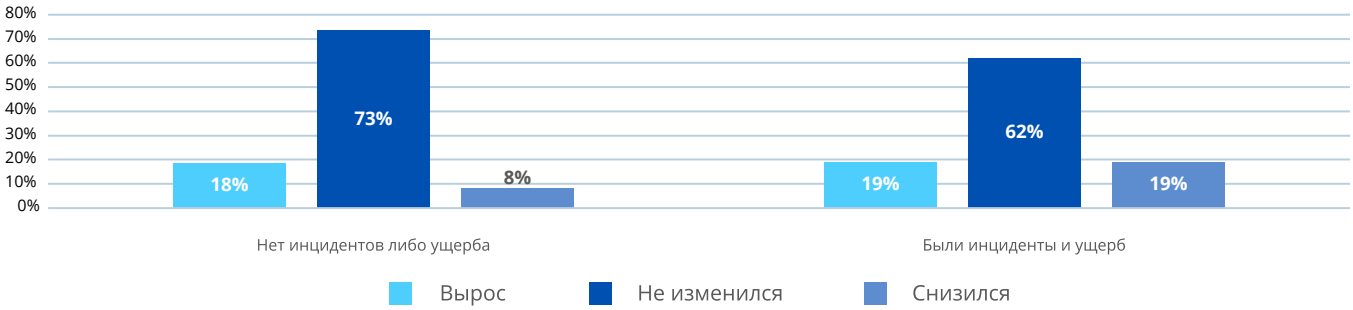


Переход к полноценному бюджетированию ИБ является ключевым фактором положительного изменения восприятия компанией защищенности от киберугроз. 61,5% респондентов, занимающихся полноценным бюджетированием ИБ и внедрения, сообщили о том, что их уровень защищенности вырос.

Компании, которые сталкиваются с инцидентами ИБ, чаще склонны более критически оценивать свое состояние, в том числе реже давать ответы «не изменился» и «снизился».

Создание культуры проактивной безопасности представляется нам одной из ключевых задач государства и индустрии в целом.

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ ПОСЛЕ КИБЕРАТАК

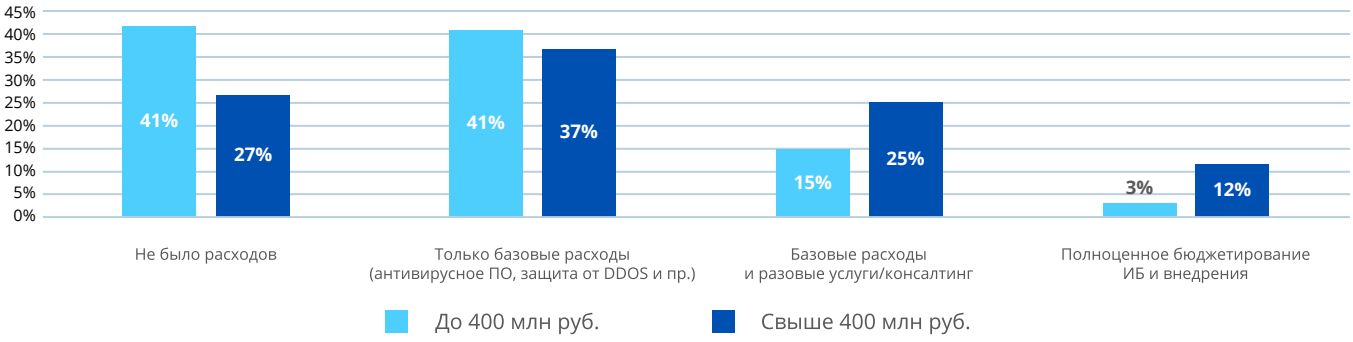


РАСХОДЫ НА ИБ

В данном блоке вопросов мы хотели изучить структуру расходов МСП на ИБ. Были исключены респонденты, которые не назвали точную сумму расходов.

Как мы уже указывали в части 1 данного исследования, значительная часть компаний сегмента МСП по-прежнему не имеет активной практики управления ИБ-рисками. При этом даже достаточно крупные компании сегмента МСП зачастую игнорируют такие риски либо ограничиваются минимальной защитой.

РАСХОДЫ НА ИБ В СРАВНЕНИИ ПО ОБЪЕМУ ВЫРУЧКИ

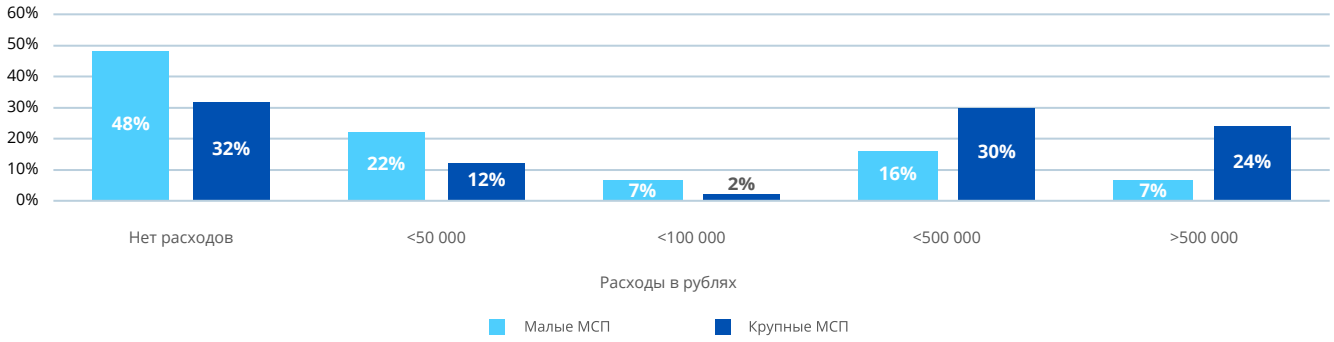


Анализ различных отраслей не показал существенной между ними разницы, в том числе между «условно высокотехнологичными» (IT, финансы, телекоммуникации, энергетика), так и «условно низкотехнологичными» (розничная торговля, ЖКХ). В частности, уровень ИБ-рисков, расходы на ИБ и наличие профильных сотрудников для большинства отраслей и групп отраслей отличаются незначительно.

В категории «IT, системная интеграция, разработка ПО, IT-консалтинг» доля ответов «не было расходов» и «только базовые расходы» превышает среднюю по выборке, опрошенные компании в этой области несут расходы на ИБ реже. Мы предполагаем, что большинство опрошенных компаний в данной сфере представляют собой небольшие предприятия, оказывающие услуги по ремонту офисной техники либо настройке ПО, и в меньшей степени занимаются разработкой программного обеспечения или высокотехнологичными задачами.

Более половины компаний МСП либо вообще не имеют расходов на ИБ, либо занижают их, либо относят их к IT. При этом доля компаний, потративших на ИБ свыше 100 тыс. руб. с ростом размера бизнеса ожидаемо растет. При этом почти ¼ крупнейших малых и средних предприятий потратила на ИБ свыше 500 000 руб.

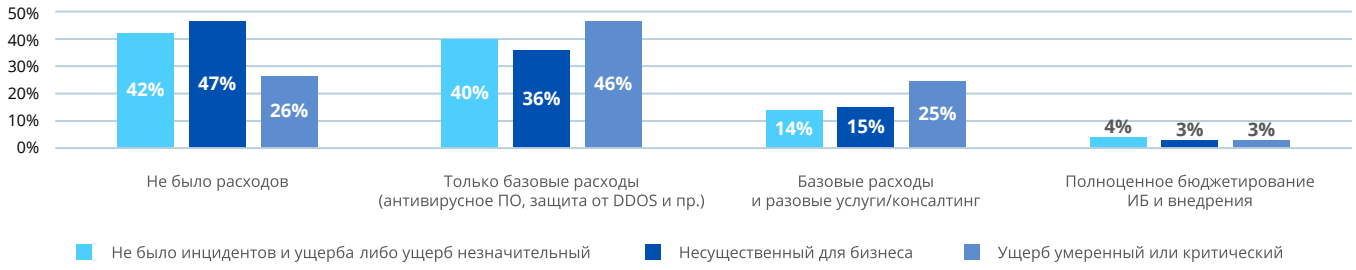
РАСПРЕДЕЛЕНИЕ РАСХОДОВ НА ИБ (В РУБЛЯХ)



Можно уверенно говорить о взаимосвязи между расходами на ИБ и наличием киберинцидентов. Компании, которые становились жертвами атак, чаще несут расходы на ИБ — среди них только 26% на момент опроса не имеют соответствующих расходов (в сравнении с 42% компаний, не имевших инцидентов или ущерба, и 47% компаний, ущерб которым был несущественным).

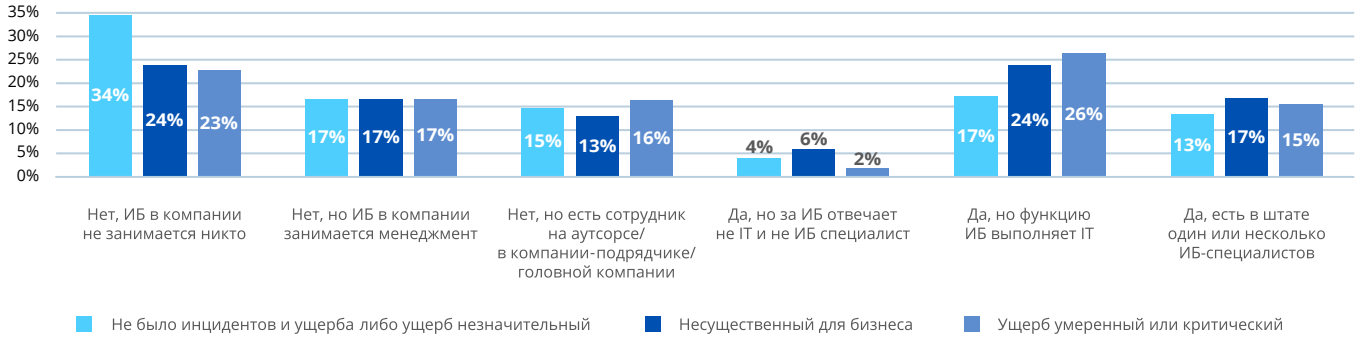
25% компаний, понесших умеренный или критический ущерб, прибегали к помощи сторонних компаний, заказывая у них отдельные услуги.

СТРУКТУРА ИБ-ИНЦИДЕНТОВ В ЗАВИСИМОСТИ ОТ РАСХОДОВ НА КИБЕРБЕЗОПАСНОСТЬ



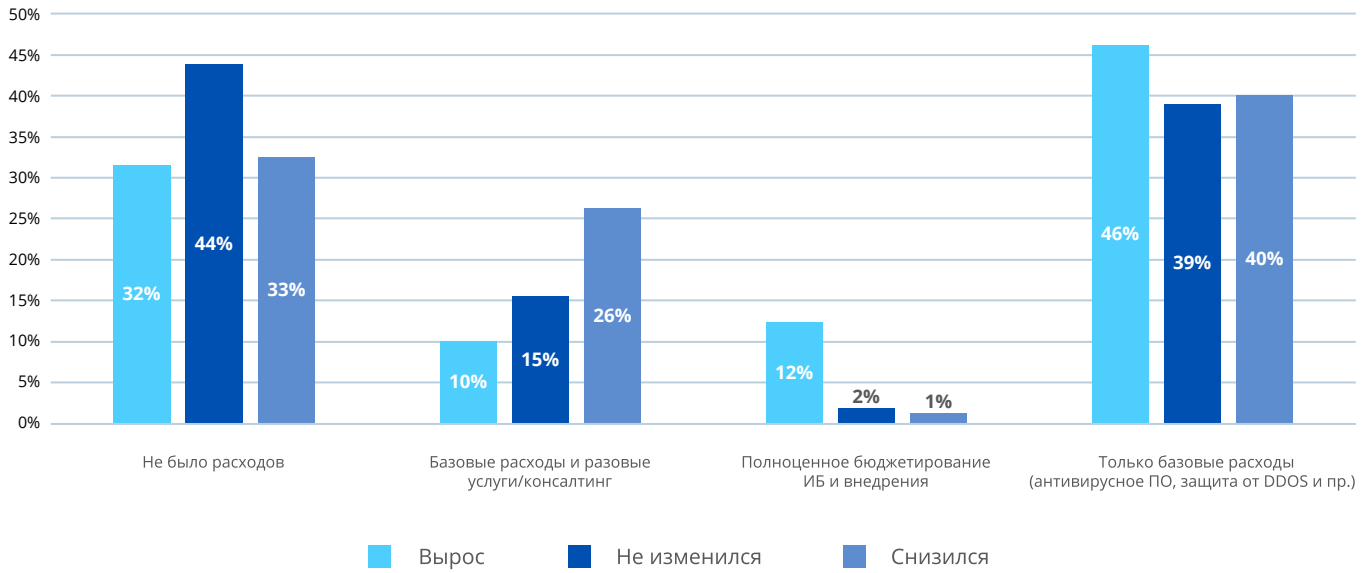
Таким образом, подтверждается гипотеза о том, что МСП действуют реактивно: большие расходы несут те, кто уже был атакован.

СТРУКТУРА ИБ-ИНЦИДЕНТОВ В ЗАВИСИМОСТИ ОТ НАЛИЧИЯ ОТВЕТСТВЕННЫХ ЗА ИБ



Даже незначительный финансовый ущерб мотивирует бизнес задуматься о необходимости совершенствования систем информационной безопасности. В то же время наличие расходов на ИБ ведет к улучшению самооценки защищенности бизнеса.

ИЗМЕНЕНИЕ САМООЦЕНКИ УРОВНЯ ЗАЩИЩЕННОСТИ МСП В ЗАВИСИМОСТИ ОТ ТИПА РАСХОДОВ НА ИБ

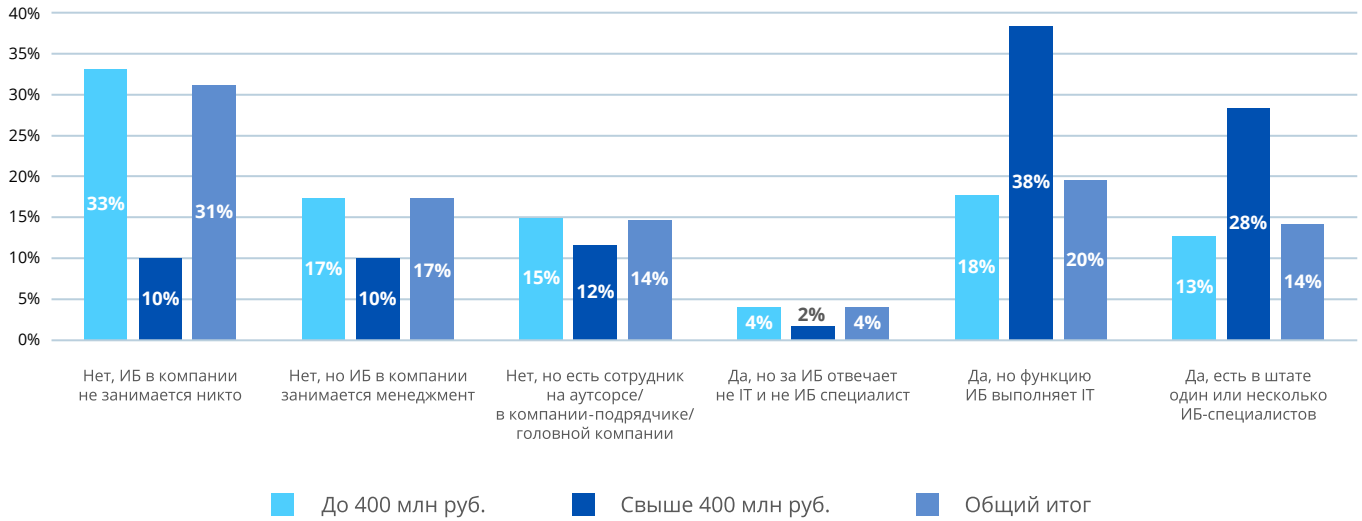


НАЛИЧИЕ ОТВЕТСТВЕННЫХ ЗА ИБ СОТРУДНИКОВ

В данном блоке вопросов мы хотели узнать, какие сотрудники отвечают за ИБ в организациях МСП.

Ситуация с наличием специалистов по ИБ схожа с ситуацией с расходами на ИБ: порядка 30% «малых МСП» не имеют в штате специалиста, ответственного за ИБ. Для «крупных МСП» наличие функции ИБ является нормой. Наиболее частым (67% случаев) является наличие ИТ-функции либо профильной ИБ-функции.

НАЛИЧИЕ ОТВЕТСТВЕННЫХ ЗА ИБ СОТРУДНИКОВ



Для микро- и малых предприятий наиболее актуальны продукты, ориентированные на защиту физлиц. Для более крупного бизнеса становятся актуальными как собственные ИБ-специалисты, так и специализированные продукты и услуги, на которые многие из них готовы тратить существенные средства.

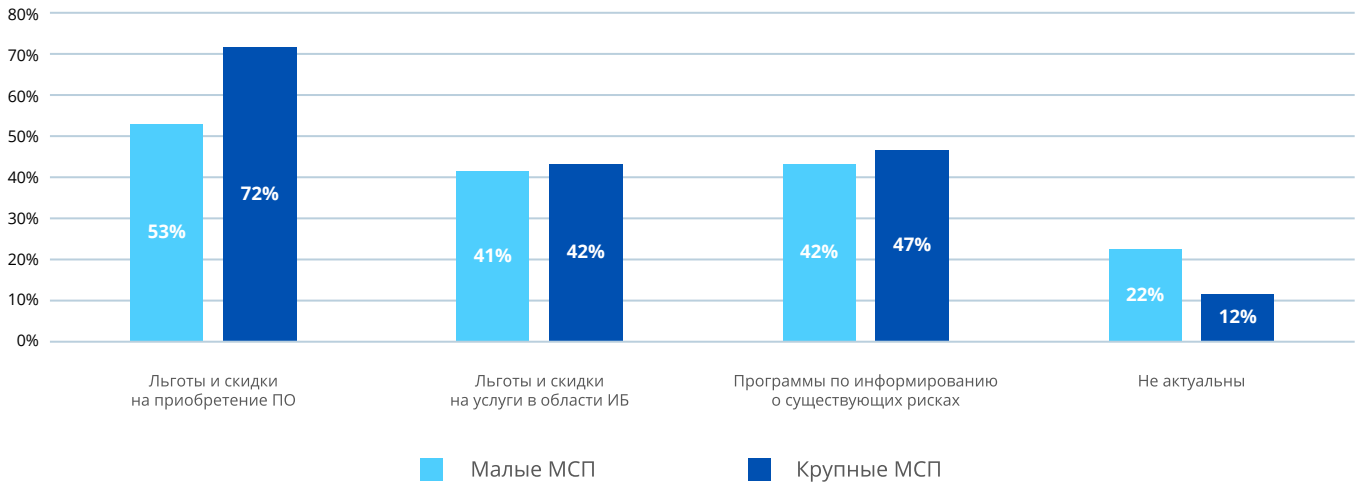
МЕРЫ ГОСУДАРСТВЕННОЙ ПОДДЕРЖКИ

В данном блоке вопросов мы опрашивали МСП на предмет необходимых им мер поддержки.

В рамках исследования возможные меры поддержки разделены на 3 основные категории: льготы на приобретение ПО, льготы на услуги в области ИБ и программы по информированию о существующих рисках.

Значительная часть респондентов выразила заинтересованность в мерах поддержки. Свыше 70% "крупных МСП" сообщили об интересе к возможным льготам на ПО, менее 10% ответили, что возможные скидки и льготы для них не актуальны.

ОЦЕНКА АКТУАЛЬНЫХ МЕР ГОСУДАРСТВЕННОЙ ПОДДЕРЖКИ ПО ТИПАМ КОМПАНИЙ (ПО ВЫРУЧКЕ)



Микропредприятия проявили меньший интерес к меркам поддержки, при этом все МСП заинтересованы в программах по информированию об угрозах.

С ростом бизнеса повышается востребованность продуктов и услуг по ИБ и их софинансирования со стороны государства.

ЧАСТЬ 3. ВЫВОДЫ И РЕКОМЕНДАЦИИ

ВЫВОДЫ

Текущая ситуация. За последние полтора года ландшафт киберугроз существенно изменился, привычные стратегии избегания киберугроз перестали работать. Общепринятые для МСП способы противодействия киберугрозам не выявлены.

Наше исследование подтверждает тенденцию последних лет: небольшие компании все чаще становятся жертвами кибератак, при этом зачастую ущерб также растет.

В России качественные услуги (и отчасти продукты) по ИБ не доступны МСП либо по причине высокой стоимости и неадаптированности для их нужд, либо по причине отсутствия у самих МСП понимания собственных потребностей и возможных угроз.

Представители малого и среднего бизнеса не всегда являются компетентными заказчиками, которые в состоянии обратиться к профессионалам и релевантно оценить киберриски и их последствия.

Невозможно объективно оценить реальный объем ущерба для сегмента МСП от инцидентов в сфере ИБ: в отличие от крупных компаний, малый бизнес крайне редко сообщает об инцидентах и при этом не является клиентом крупных компаний в сфере ИБ, собирающих данные о защищенности своих клиентов.

Прогнозы и ожидания. При сохранении активной массовой цифровизации, текущей политической обстановки и фрагментированности правового поля динамика роста числа кибератак на российский бизнес сохранится. Основная часть усилий государства и крупных игроков рынка пока направлена на защиту ключевых объектов инфраструктуры, финансовой системы и крупного бизнеса.

МСП занимают всего 20% экономики России (для сравнения, в Китае — свыше 60%). Президентом России Владимиром Путиным неоднократно ставилась задача довести долю предприятий малого и среднего бизнеса в стране до 40%, чтобы обеспечить стабильный рост российской экономики. Киберугрозы МСП будут расти, и для достижения озвученных целей важно уже сейчас адекватно оценивать защищенность этого сегмента и принимать меры по ее улучшению.

Регулярные утечки баз данных, содержащих персональные данные граждан, продолжатся без введения оборотных штрафов за их допущение и укрепления защищенности бизнеса от киберугроз.

Решение проблемы кадрового голода в ИБ в обозримом будущем крайне затруднено: подготовка квалифицированного специалиста на базе высшего образования занимает не менее 4 лет, на базе отдельных курсов — не менее года. Уже сейчас проблема поиска специалистов на рынке ограничивает МСП в возможности их найма: компетентных специалистов на рынке не хватает, а многие выпускники профильных ВУЗов не работают по специальности.

Ключевая причина наблюдаемого дефицита кадров — низкий уровень зарплат в ИБ, в том числе в госсекторе. В дальнейшем это приведет к «перетеканию» наиболее квалифицированных кадров как на коммерческий рынок труда, так и на мировой рынок. Спрос на российских специалистов по ИБ по всему миру будет расти. Мы предполагаем, что данная проблема сохранится и требует серьезного внимания государства.

РЕКОМЕНДАЦИИ

Субъектам МСП, ранее не сталкивавшимся с ИБ, мы в первую очередь рекомендуем оценить сценарии, при которых киберриски могут нанести критический ущерб их бизнесу. В случае если такие сценарии возможны и ущерб от них значительно превышает любой возможный бюджет на ИБ, мы настоятельно рекомендуем как минимум воспользоваться услугами компетентных консультантов с рынка. Также имеет смысл разобраться, как устроен рынок услуг в ИБ.

Ситуация, когда ИБ-риски не несут значимой угрозы бизнесу вполне возможна для микропредприятий, не имеющих развитой IT-инфраструктуры. В таких случаях мы предлагаем ограничиться антивирусным ПО. Большинству представителей среднего бизнеса мы настоятельно рекомендуем хотя бы оценить возможные риски и стоимость построения или оптимизации ИБ-процессов.

Лучшей практикой для МСП мы считаем не построение защиты «от всего» а безопасность, ориентированную на угрозы бизнесу. С нашей точки зрения, первостепенным для бизнеса является определение ключевых связанных с ИБ рисков и защита от них.

Государству необходимо заняться формированием культуры информационной безопасности у бизнеса. В условиях ограниченности бюджета МСП без роста компетенций бизнеса возможности эффективной защиты от киберугроз будут ограничены, а любые меры поддержки окажутся недостаточно эффективными. На наш взгляд, именно образовательная функция государства является ключевой.

Мы считаем возможным сформировать государственные меры поддержки для МСП, стимулирующие покупку российских решений в сфере кибербезопасности. Данные меры помогут бизнесу не только сократить расходы на ПО, но и развить привычку заниматься ИБ.

Подготовка ИБ-специалистов требует повышенного внимания. На период перестройки ВУЗами образовательных программ необходимо рассмотреть возможность временного трудоустройства/практики выпускников онлайн-курсов по ИБ и публичного рейтингования таких курсов.

Государственное сертифицирование в данном случае не только не решит проблему, а скорее усугубит ее. К примеру, некоторые существующие государственные сертификаты в области ИБ для бизнеса (например, ТЗКИ) уже давно не воспринимаются на рынке как подтверждение качества работы компании. Скорее, необходимость их получения рассматривается как единоразовый «налог» на новые ИБ-компании при том, что наличие такого сертификата, как правило, не говорит о статусе и компетенциях компании.

Общий вывод: для повышения доступности компаниям МСП продуктов и услуг по ИБ необходимы комплексный подход и существенные изменения на уровне государства.

Для решения проблемы в меняющейся среде и сложном внешнеполитическом окружении необходима долгая, последовательная и комплексная работа. **Ни государство, ни бизнес, ни ИБ-индустрия не смогут решить эту проблему в одиночку.**

В дальнейшем регулярное проведение такого рода исследований позволит систематически проводить оценку защищенности сегмента МСП, прозрачно и подробно оценивать происходящие там изменения. Привлечение большего числа респондентов позволит более качественно оценить потребности бизнеса по ИБ в разрезе как отдельных отраслей, так и отдельных регионов и принять меры по совершенствованию рынка ИБ в России.

ОБ ОРГАНИЗАЦИЯХ

Автономная некоммерческая организация «Агентство стратегических инициатив по продвижению новых проектов (АСИ)» создана распоряжением Правительства России от 11 августа 2011 года.

Наблюдательный совет АСИ возглавляет Президент России Владимир Путин.

Агентство поддерживает проекты, направленные на системные изменения в сфере повышения качества жизни, экологии, образования и подготовки кадров, регионального и городского развития, разработки новых технологий и поддержки бизнес-проектов.

Среди ключевых инициатив АСИ — Национальный рейтинг состояния инвестиционного климата в регионах, Рейтинг качества жизни, Национальная социальная инициатива, Национальная кадровая инициатива, платформа для обмена лучшими практиками «Смартека».

ASI.RU

ООО «Третья Сторона» — российский независимый технологический стартап, зарегистрированный в особой экономической зоне Иннополис. Площадка 3side объединяет множество опытных специалистов в области ИБ.

Своей целью компания называет создание конкурентного, надежного и прозрачного рынка услуг по информационной безопасности в России.

3SIDE.ORG

КОНТАКТНАЯ ИНФОРМАЦИЯ

РАЦЕЕВА СВЕТЛАНА

Директор практик Дивизиона «Технологии и предпринимательство», АСИ

ss.ratceeva@asi.ru

БОЧКАРЕВ АНТОН

Основатель ООО «Третья Сторона».

adb@3side.org

8 800 222 1337

t.me/TG_3side