# ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ МАЛЫХ И СРЕДНИХ ПРЕДПРИЯТИЙ: СОВРЕМЕННЫЕ УГРОЗЫ И НЕОБХОДИМОСТЬ ЗАЩИТЫ

**Гофурова Лазиза Жасур кизи**
*студентка Ташкентского университета информационных технологий имени аль-Хорезми*
lazizagofurova52@gmail.com
+998935117409

**Введение:** Информационная безопасность (ИБ) стала неотъемлемой частью устойчивого развития бизнеса в цифровую эпоху. Если крупные корпорации давно инвестируют значительные ресурсы в киберзащиту, то малые и средние предприятия (МСП) нередко считают, что их небольшой масштаб уберегает от внимания киберпреступников. Однако статистика и реальные инциденты опровергают это заблуждение. Согласно недавним исследованиям, в 2023 году инциденты информационной безопасности произошли у 45% российских компаний МСП, при этом 30% пострадавших компаний оценили ущерб как умеренный или критический. Подобные показатели подтверждаются и за рубежом: ежегодно с киберинцидентами сталкиваются около 50% малых и средних компаний в Великобритании. Тем не менее, до 40% небольших фирм вообще не выделяют бюджет на ИБ, ограничиваясь минимальными мерами. В результате малый бизнес все чаще становится целью атак злоумышленников, испытывая те же угрозы, что и крупные организации. Финансовые потери от утечек данных или кибератак могут оказаться для небольшой компании несопоставимо тяжелее, вплоть до остановки деятельности. Введение базовых практик ИБ даже при ограниченных ресурсах способно существенно снизить эти риски. В данном тезисе представлен анализ современных киберугроз, с которыми сталкиваются малый и средний бизнес, рассмотрены примеры инцидентов и их последствия, а также обоснована необходимость внедрения мер информационной безопасности в МСП на основании актуальных данных и источников.

**Современные киберугрозы для МСП**

Актуальный ландшафт киберугроз демонстрирует, что малые и средние предприятия подвержены самому широкому спектру атак. Вредоносное

программное обеспечение (malware) остается одной из главных опасностей. По данным анализа «Лаборатории Касперского», в первом квартале 2024 года количество заражений ИТ-систем МСП возросло >5% по сравнению с аналогичным периодом 2023 года. Наиболее распространены атаки троянских программ: злоумышленники внедряют их под видом легитимного софта, что затрудняет обнаружение и позволяет обходить традиционные средства защиты. Особую тревогу вызывают программы-вымогатели (ransomware), шифрующие данные и требующие выкуп. Исследования показывают, что 82% всех атак вымогателей нацелены на компании с числом сотрудников менее 1000, то есть преимущественно на средний и малый бизнес. Многие МСП не обладают резервными ресурсами для восстановления: по опросам, до 75% небольших фирм не смогли бы продолжать работу после серьёзной атаки вымогателей. Таким образом, угрозы типа ransomware способны буквально поставить крест на дальнейшем существовании незащищённого предприятия.

Социальная инженерия и фишинг – ещё одна массовая угроза, зачастую направленная именно на сотрудников небольших компаний. Киберпреступники исходят из предположения, что в малых фирмах меры защиты и осведомленность персонала слабее, чем в корпорациях. В результате сотрудники МСП подвергаются атакам социального инжиниринга на 350% чаще, чем работники крупных компаний. Фишинговые рассылки по электронной почте, мессенджерам и соцсетям пытаются обманом выудить учетные данные или заражают устройства. Человеческий фактор становится слабым звеном: неосторожность персонала способна привести к серьезному инциденту. Например, получение сотрудником письма с ссылкой на поддельную страницу входа популярного сервиса может привести к компрометации учетных записей и утечке конфиденциальных данных организации.

Рис. 1: Пример фишингового веб-сайта, имитирующего страницу входа известного сервиса доставки. Невнимательный сотрудник, введя здесь свои учетные данные, передает их злоумышленникам, что может привести к компрометации корпоративной системы. Малые компании, не внедрившие должных средств киберзащиты (например, фильтров и 2FA), особенно уязвимы к таким атакам. Помимо внешних атак, внутренние угрозы также актуальны для МСП. Небольшой коллектив не гарантирует отсутствия инсайдерских инцидентов. Согласно исследованию компании SearchInform,

100% опрошенных компаний МСП в 2023 году столкнулись с внутренними инцидентами безопасности — утечки информации, мошенничество сотрудников, использование ресурсов в личных целях и пр. Утечки конфиденциальных данных (клиентской базы, финансовых документов, ноу-хау) могут происходить как вследствие внешнего взлома, так и по вине персонала. В отличие от корпораций, где над предотвращением утечек трудится целый отдел информационной безопасности, у малого бизнеса зачастую нет выделенных специалистов. Поэтому невыявленная вовремя утечка может обернуться банкротством небольшой фирмы. Кроме того, корпоративное мошенничество распространено даже в малых компаниях: в 2023 году 50% российских МСП отмечали случаи мошеннических действий сотрудников (например, откаты, «работа на конкурентов»). Каждый второй такой инцидент – это прямые финансовые потери и ущерб репутации, особенно опасные для компаний с низким «запасом прочности».

Таким образом, современные угрозы для малого и среднего бизнеса разнообразны: от вредоносных программ и хакерских атак (прямо угрожающих ИТ-инфраструктуре) до социальной инженерии (направленной на сотрудников) и злоупотреблений изнутри. Небольшие организации, ошибочно полагающие, что останутся вне поля зрения атакующих, на практике становятся удобной мишенью. Злоумышленники используют факт, что 51% небольших компаний не имеют никаких мер киберзащиты, и способны нанести удар, последствия которого непропорционально тяжелы для бизнеса малого масштаба.

**Примеры инцидентов и их последствия**

Рассмотрим несколько показательных инцидентов, иллюстрирующих важность ИБ для МСП. Один из распространенных внешних сценариев – атака вымогателя на небольшую фирму. Так, в феврале 2022 года небольшая производственная компания подверглась атаке шифровальщика, парализовавшей работу её серверов на несколько дней (условный пример, основанный на совокупных чертах реальных случаев). У предприятия не оказалось актуальных резервных копий, и встала дилемма: потерять критически важные данные или заплатить выкуп. Подобно более чем половине пострадавших малых фирм (51%), компания была вынуждена заплатить киберпреступникам. Но даже после этого восстановление системы заняло время, клиенты на дни остались без сервиса, что нанесло удар по деловой репутации. Исследования показывают, что 55% клиентов теряют

доверие к компании после утечки или взлома, поэтому такой инцидент грозит потерей части бизнеса в будущем. К сожалению, подобные истории нередки: почти 40% небольших фирм сообщают, что в результате кибератаки теряли важные данные. Этот пример демонстрирует, что отсутствие надлежащей подготовки (резервирования данных, планов реагирования) делает малый бизнес чрезвычайно уязвимым.

Другой кейс – внутренний инцидент, связанный с утечкой информации. В опубликованном случае из практики аутсорсинговой ИБ-компании, небольшая фирма розничной торговли столкнулась с попыткой кражи клиентской базы сотрудником. Менеджер по продажам, сговорившись со знакомым в фирме-конкуренте, планировал скопировать конфиденциальный список клиентов на внешний носитель и передать его за вознаграждение. Попытка была вовремя выявлена аналитиком благодаря установленной DLP-системе (системе предотвращения утечек), что позволило пресечь инсайдерскую угрозу. Здесь наглядно проявляется ценность средств мониторинга и политики контроля доступа: если бы не предпринятые защитные меры, компания потеряла бы коммерчески ценную информацию, дав конкуренту преимущество и нанеся ущерб своим будущим доходам. Подобный инцидент также подчеркнул риск доверия персоналу на словах – требуются технические средства контроля, даже если коллектив невелик.

Стоит отметить и организационные последствия киберинцидентов для МСП. В отличие от гигантов, обладающих резервными фондами и дублированными системами, малые предприятия могут не восстановиться после тяжелого инцидента. Например, по данным опросов, каждая четвертая небольшая компания (25%) после серьезной кибератаки находится на грани закрытия, а некоторые прекращают деятельность в течение месяцев после утечки данных (данные различных исследований, отраженные в совокупной статистике). Даже менее катастрофичные на первый взгляд события – простои ИТ-систем из-за вирусов или DDoS-атак – непосредственным образом бьют по бизнес-процессам. Если, скажем, на день будет недоступен сайт интернет-магазина или выйдет из строя почтовый сервер фирмы, коммерческие и операционные потери за этот период для малого бизнеса будут весьма ощутимы. Исследование Gartner еще в 2014 году оценивало среднюю стоимость простоя бизнеса в $5600 в минуту, а в 2024 году отраслевые опросы показали, что даже несколько минут простоя могут полностью остановить работу организации и привести к серьезным убыткам.

Для МСП даже десятки тысяч долларов потерь могут быть критичными. Таким образом, каждый конкретный инцидент (будь то внешняя атака или внутренняя утечка) несет не только прямые затраты на ликвидацию последствий, но и косвенные убытки: простой бизнес-процессов, штрафы за несоблюдение закона о защите данных, падение доверия клиентов, отток контрактов. Все это подтверждает: проактивная защита информации – вопрос выживания и стабильности бизнеса.

**Обеспечение безопасности при ограниченных ресурсах**

Перед малым и средним бизнесом стоит непростая задача: как защититься от перечисленных угроз, не располагая ни многомиллионными бюджетами, ни штатом из десятков ИБ-специалистов. Тем не менее, существует комплекс мер, реализация которых по силам даже организациям с ограниченными ресурсами. Прежде всего, важно изменение отношения: осознание руководством реальности киберрисков для любой компании. Примечательно, что 59% владельцев малого бизнеса без мер защиты считают свой бизнес "слишком маленьким для атаки", что свидетельствует о недооценке угроз. Преодолев этот миф, можно планомерно выстраивать систему безопасности в рамках доступных средств.

Приоритетные меры кибербезопасности для МСП можно условно разделить на организационные и технические. К организационным относится формирование культуры безопасности и обучение персонала. Даже без выделенной должности инженера по безопасности, каждый сотрудник должен владеть базовыми знаниями: как распознать фишинговое письмо, почему нельзя использовать простые пароли или открытые Wi-Fi для работы, как сообщать о подозрительных событиях. Регулярные тренинги и инструктажи повышают общий уровень киберграмотности и снижают шансы успешной атаки через человеческий фактор. Например, обучение сотрудников правилам обращения с паролями, практикам антифишинга и безопасной работы в интернете существенно уменьшит риск инцидентов. В поддержку этому, компании могут внедрять политику информационной безопасности: регламенты, четко прописывающие, какие действия запрещены (подключение личных устройств без проверки, установка софта без разрешения ИТ-специалиста и др.). Как показывает практика, во многих небольших организациях таких регламентов нет вовсе, однако их введение не требует больших затрат, но способствует дисциплине и осознанию важности ИБ.

Со стороны технических решений первоочередной шаг – внедрение базовых средств защиты. К ним относятся современное антивирусное/Endpoint Protection ПО, сетевые экраны (фаерволы) для фильтрации трафика, спам-фильтры и системы фильтрации фишинговых писем для корпоративной почты. Эти инструменты сейчас доступны и в виде недорогих облачных сервисов, и как встроенные решения в популярных ОС, поэтому даже небольшой компании по силам их развернуть. Следующий критичный элемент – резервное копирование данных. Регулярное создание резервных копий важной информации должно стать рутиной, позволяющей восстановить работу после сбоя или шифровальщика. Желательно использовать правило 3-2-1 (три копии, на двух разных носителях, одна – вне офиса/в облаке) для повышенной надежности. Многие тяжелые последствия атак можно смягчить, если имеется актуальный бэкап: например, вместо оплаты выкупа можно восстановить данные из копий.

Контроль доступа и учетных записей – еще одна зона внимания. Даже в небольшой компании важно распределять права доступа по принципу минимальной достаточности: сотрудник должен иметь доступ лишь к тем данным и системам, которые необходимы ему для работы. Регулярный аудит учетных записей и привилегий позволит избежать ситуации, когда у уволенного сотрудника остался активный логин или стажер имеет права администратора системы. Простое наведение порядка в учетных записях закрывает множество потенциальных "дыр". Помимо этого, современные облачные сервисы предлагают инструменты мониторинга активности пользователей (CASB – брокеры безопасности доступа к облаку), которые помогают обнаружить аномальные действия (например, массовое скачивание данных не в рабочее время). Для МСП, активно использующих облачные решения (почту, хранилища, SaaS), такие инструменты часто включены в бизнес-тарифы и стоит их задействовать.

Отдельно следует подчеркнуть многофакторную аутентификацию (MFA) – один из самых эффективных и недорогих способов повысить безопасность учетных записей. Даже если злоумышленник узнает пароль сотрудника (через фишинг или утечку), требование второго фактора (смс-код, приложение, аппаратный токен) может сорвать атаку. По опросам, лишь 20% небольших фирм внедрили MFA для своих систем, тогда как для критичных сервисов это должно стать нормой. Бесплатные решения (Google Authenticator, Microsoft Authenticator и др.) делают MFA доступной каждому.

Наконец, оптимальным решением при нехватке собственных экспертов является привлечение внешних специалистов или аутсорсинг ИБ. Многие МСП сегодня пользуются услугами провайдеров, предлагающих защиту "как сервис": от поддержки сетевой инфраструктуры до мониторинга событий безопасности. Согласно исследованию, 40% компаний с годовым оборотом до 2 млрд руб. привлекают сторонние фирмы для обеспечения должного уровня защиты. Передача функций ИБ аутсорсеру позволяет малой компании получить квалифицированный контроль за своим периметром без найма штатной команды. Например, аутсорсинговый SOC (центр оперативного реагирования) будет отслеживать атаки и инциденты 24/7, что самостоятельно МСП организовать затруднительно. Аналогично, существуют сервисы по аудиту уязвимостей, тестированию на проникновение, обучению персонала онлайн – все это доступно на контрактной основе. Конечно, даже при аутсорсинге ответственность за безопасность лежит на руководстве компании: важно выбрать надежного партнера и соблюдать его рекомендации.

В целом, комплексный подход к ИБ для малых и средних предприятий включает: 1) формирование осведомленности и политики внутри компании; 2) внедрение базовых технических средств защиты (антивирус, фаервол, резервирование, MFA); 3) регулярный мониторинг и аудит (самостоятельно либо через подрядчиков); 4) план реагирования на инциденты (заранее продумать, что делать в случае взлома или утечки). Даже при ограниченном бюджете реализация этих шагов возможна поэтапно и принесет несоизмеримо большую пользу, чем полное отсутствие мер. Напомним, что в 4% небольших компаний ИБ уже выделена отдельной статьей бюджета – эти предприятия понимают стратегическую важность защиты информации. Остальным же МСП необходимо перенимать лучший опыт, чтобы не стать легкой добычей для киберпреступников.

**Заключение:** Малые и средние предприятия сегодня так же зависимы от информационных технологий, как и крупные корпорации, а значит – так же уязвимы перед киберугрозами. Проведенный анализ показывает, что ни один бизнес не слишком мал для кибератаки: злоумышленники активно эксплуатируют недостаток ресурсов и опыта в сфере ИБ у небольших компаний. Типичные угрозы – от вирусных эпидемий до целевых фишинговых атак и внутренних утечек – уже приводят к серьезным инцидентам в секторе МСП, нанося финансовый и репутационный ущерб.

При этом масштаб потерь для малых предприятий относительно их оборота зачастую критичнее, ставя под угрозу само продолжение бизнеса. Игнорирование информационной безопасности перестает быть вариантом даже при скромном бюджете.

Уделяя внимание кибербезопасности, малые компании инвестируют в свою устойчивость и доверие клиентов. Реальные примеры показывают, что простые шаги (резервное копирование, обучение персонала, обновление софта, MFA) могут предотвратить катастрофический сценарий либо существенно смягчить последствия инцидента. Да, построение системы защиты – это непрерывный процесс, требующий и времени, и дисциплины, однако наградой служит непрерывность бизнес-процессов и сохранность ключевых данных. В современных условиях конкурентоспособность во многом определяется надежностью: партнеры и клиенты предпочитают иметь дело с теми, кто защищает их информацию. Таким образом, внедряя меры информационной безопасности, даже небольшая фирма получает стратегическое преимущество – уверенность в завтрашнем дне и возможность сконцентрироваться на развитии, не отвлекаясь на ликвидацию предотвратимых чрезвычайных ситуаций.

Подводя итог, информационная безопасность для МСП – не роскошь и не дань моде, а необходимый элемент управления рисками. Сочетание разумных технических решений и культивирование осознанности сотрудников позволит малому и среднему бизнесу выстроить эффективную оборону, соизмеримую с угрозами цифровой эпохи. Безопасность информации должна стать таким же привычным аспектом управления компанией, как учет финансов или забота о качестве продукции. Только в этом случае можно минимизировать угрозы и обеспечить долгосрочное процветание организации в условиях стремительно развивающегося цифрового мира.

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Лаборатория Касперского. «Отчёт об угрозах для бизнеса 2023–2024» Group-IB. «Ransomware Uncovered 2023»
2. Национальный исследовательский университет «Высшая школа экономики». «Киберугрозы для малого бизнеса» Cisco. «SMB Cybersecurity Report»
3. Microsoft Security Blog. «Small Businesses Are a Big Target for Cybercrime»
Gartner Research. «The Cost of IT Downtime»
4. IBM X-Force Threat Intelligence Index 2024SearchInform. «Внутренние угрозы информационной безопасности: кейсы и анализ»