

Забывшие в дальнем углу шкафа десятки страниц технической информации и запутанной терминологии? Нет, это не та политика безопасности, которой надлежит придерживаться в вашей организации. Кстати, в сегодняшнем выпуске мы будем говорить не о таком документе. Вместе с экспертом в области безопасности и рисков, работающим в International Media Support, Джозефом Хамудом мы объясним, **как разработать для вашей редакции простую, эффективную и применимую политику безопасности.**

Джозеф Хамуд

эксперт в области безопасности и рисков в International Media Support



Как внедрить концепцию безопасности нашей команды, не создавая панику?

Команде следует объяснить, что безопасность нужна для того, чтобы мы могли продолжать работать в любой ситуации, а для этого необходимо понять, что именно может мешать бесперебойности нашей деятельности. Важно увязывать риски и безопасность с непрерывностью бизнеса, ведь именно в этом, по сути, и кроется причина разработки такой политики. Документ должен «сообщить» нам, на каких угрозах следует сосредоточить внимание, и как их устранять.

Как составляется политика в области безопасности?

Самый большой риск политики в области безопасности — слишком длинный и затрудненный для восприятия документ. Если привлечь кого-то, кто составит этот документ, чтобы тот лежал где-то на полке и его можно было иногда показывать донорам, то проблему эту не решит. **Политика в области безопасности должна быть полезным и практическим документом, а не бюрократической формальностью.** Важен не объем документа, а то, что эта политика именно наша. Мы всегда можем ее скорректировать по мере развития организации. Мониторинг и пересмотр политики можно осуществлять ежегодно, привлекая к этой задаче команду.

Для начала следует собраться вместе с командой и определить, что именно угрожает нашей работе и возможности продолжать операции. Важно, чтобы эти риски отражали нашу действительность, а не были предположениями людей извне. Дискуссия должна быть искренней и раскрывать то, что нас по-настоящему тревожит и беспокоит. Это могут быть аспекты, связанные с менеджментом, внутренними конфликтами, внешними нападками, политической ситуацией, правовыми проблемами. Хотя некоторые из этих проблем чувствительные, мы должны осознать их и решить, иначе они продолжат усугубляться и однажды обернутся кризисом.

Когда мы поймем, что именно может сказаться на нашей работе, то упорядочим все эти аспекты в зависимости от их срочности. Затем надо будет искать подходящие решения каждой проблеме, чтобы эффективно устранять их.

Следующий шаг — определить другие заинтересованные стороны. Какие бы проблемы мы ни обнаружили, мы не одни. Надо понимать, какие у нас союзники и какая роль им отводится. Далее важно наладить связи с ними, пообщаться с ними перед возникновением возможного кризиса.

Надлежит учитывать также этические и нравственные аспекты, такие как обязательство о заботе, гендерная инклюзия, то есть вещи, которые мы могли упустить в самом начале. Затем мы сосредоточимся на разработке запасного плана для наиболее острых/злободневных рисков.

Самый важный аспект этого процесса — работа команды, поэтому и процесс, и результаты становятся гораздо более значимыми. Это будут наши идеи о том, как защитить нашу организацию, и, таким образом, разрабатываемая политика будет практичной и привязанной к нашим реалиям.

Роль этой политики — своевременно подготовить нас к возможным угрозам, ведь только подготовка поможет нам обеспечить непрерывность работы организации.

Когда наступает подходящее время приступить к работе над нашей политикой в области безопасности?

Безусловно, заняться этим следует когда все спокойно. Планировать следует до кризиса — невозможно вести подготовку во время борьбы, ведь тогда мы только будем реагировать, однако суть подготовки именно в том, чтобы действовать на опережение.

Необходимо ли некое пособие или руководство по осуществлению политики в области безопасности?

Да, вам потребуется такое руководство, однако заниматься его составлением должен не эксперт, который разработает политику вместо нас или же предоставит нам некий типовый образец, который мы скопируем. В процессе анализа рисков рассматриваются пять важных аспектов: операционный, политический, правовой, финансовый и репутационный. Команда обсудит каждую из этих областей, но тот, кто ведет дискуссии, может направлять разговор, или же высказывать свое мнение.

Кто входит в состав команды по управлению кризисом?

Выбирая команду, которая займется управлением кризиса, важно отобрать тех, кто хорошо знает организацию и внутренние процессы, при этом занимая ими должность значения не имеет. Нам нужны и технически подкованные люди, а этим утверждением мы сейчас оспариваем сказанное выше, но в данном случае не нужно, чтобы, к примеру, IT-эксперты входили в состав организации. Эти люди могут помочь нам со специфической задачей, поэтому нет необходимости включать их в состав команды по управлению кризисами.

Аналогичным образом и для получения общих консультаций в случае чрезвычайных ситуаций можно обратиться к внешнему эксперту. Это не означает, что команда становится больше: в ее состав и далее будут входить основные люди организации, но в нашем распоряжении будут и дополнительные контакты, к которым мы сможем прибегать в случае необходимости.

Команда по урегулированию кризиса создается после анализа и оценки рисков на основе выводов и выявленных потребностей, ведь только на данном этапе мы поймем, сколько людей нам нужно, и к каким людям извне нам необходимо обратиться.

Что происходит после кризиса?

После кризиса следует проанализировать, что именно произошло, что можно было сделать лучше, что оказалось полезным на практике, какие инструменты мы использовали и каким образом, как следует актуализировать нашу политику. Промехи будут всегда, ведь кризисы динамичные. Вне зависимости от степени нашей подготовки останутся и «слепые углы».

Сколько информации о кризисе должны получать наши работники, наши сотрудники и наша аудитория?

В команде есть менеджеры, управляющие кризисом, и есть люди, на которых кризис сказывается. Надо понимать, кого может затронуть кризис, как следует адаптировать коммуникацию в зависимости от каждой группы.

Членам команды, которые не задействованы в урегулирование кризиса, но которые затронуты им прямым образом, следует сообщить важные для них аспекты, чтобы они могли принимать решения. К примеру, в случае кибератаки или рейда в офис, команде следует сообщить об этом, чтобы персонал оставался дома. Необходимо применять коммуникационную стратегию для команды, чтобы люди получали уведомления регулярно (ежедневно, раз в два дня или же реже, в зависимости от обстоятельств). Аудитории однако не нужно сообщать информацию каждые два дня. Может оказаться достаточно публичного сообщения о случившемся, о том, как это нас затрагивает, какие сервисы изменяются, и т. д.

Вот почему важным шагом в анализе рисков станет и анализ вовлеченных партнеров по отношению к рискам.

Как правильно составить бюджет, чтобы незамедлительно реагировать на потребности в области безопасности?

Речь идет о том, каким образом безопасность и подготовка к кризису связаны с организационным развитием. Все планы по обеспечению непрерывности операционной деятельности должны быть включены в бюджет по развитию.

В данном случае важная роль отводится партнерам организации, которым следует сообщить, что таким образом мы инвестируем в безопасность организации и в продолжение нашего развития. К примеру, развитие IT-инфраструктуры обеспечивает нам не только защиту — это означает, что мы на самом деле инвестируем в безопасность и потенциал организации. Речь не только о безопасности — речь о потребности в организационном развитии.

В случае реального кризиса поступит дополнительная поддержка от различных игроков, но если у нас уже есть определенные планы и мы точно знаем, что нам нужно, то сможем отреагировать незамедлительно и выдвинуть ясные требования.

Итак, с одной стороны у нас есть бюджет на развитие, а с другой стороны у нас есть экстренные ситуации, в случае которых мы прибегнем к чрезвычайным фондам.



Возможности!

Редакции могут получить гранты на развитие институционального потенциала. К числу приемлемых для финансирования видов мероприятий относятся инициативы по укреплению цифровой безопасности, а также по предупреждению выгорания и поддержке психического здоровья издательским командам. Узнай подробности [здесь](#).



Прости о помощи!

Если сталкиваешься с постоянным стрессом и тревожностью, можешь обратиться за бесплатной и конфиденциальной консультацией психолога через [этот чат-бот](#) или заполнив [этот бланк](#). В течение 48 часов с тобой свяжется специалист.

Если эти материалы тебе понравились, тогда рекомендуем нашу электронную рассылку и своим коллегам по журналистскому цеху. Отзывы и обратная связь помогут нам стать лучше. Напиши свое мнение об электронной рассылке и отправь его нам на следующий адрес ari@ari.md.