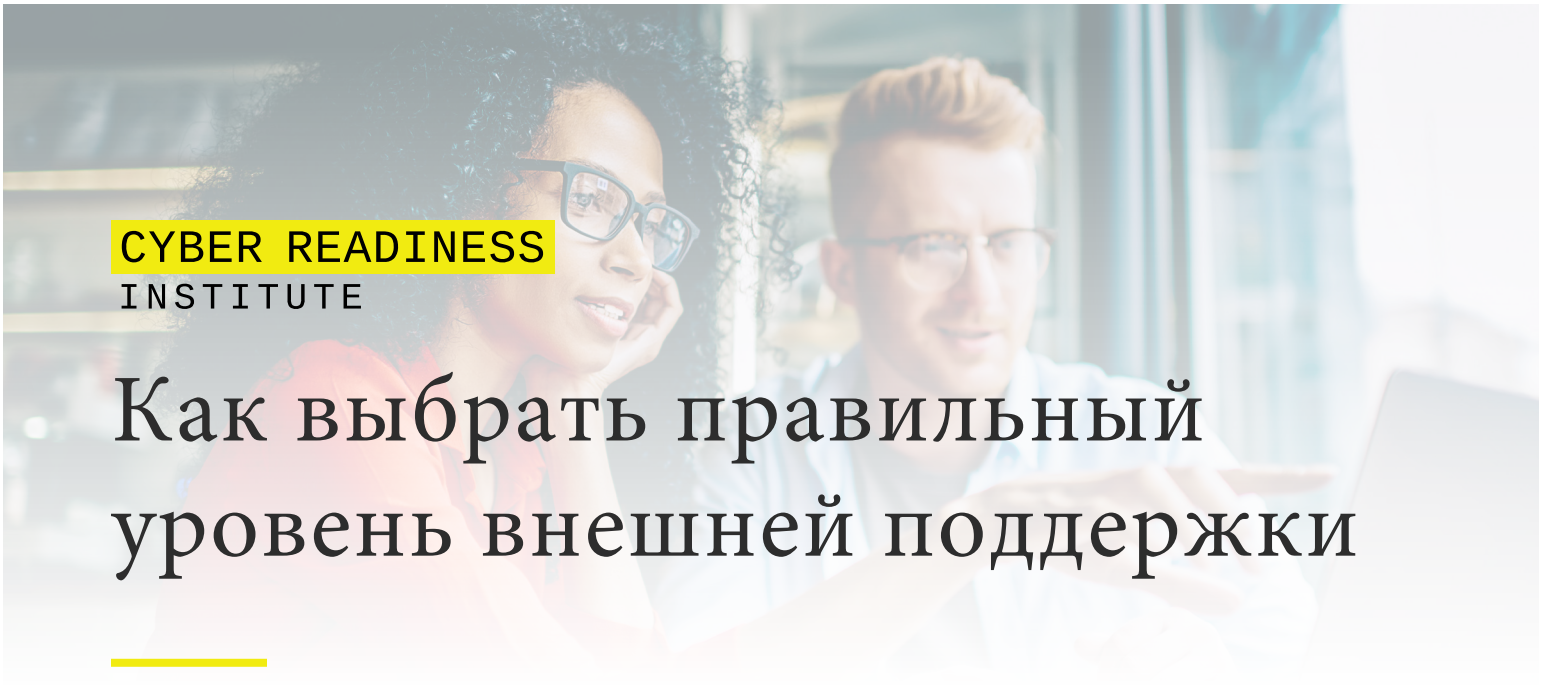

CYBER READINESS
INSTITUTE

Как выбрать правильный уровень внешней поддержки

Это третья часть из серии руководств, состоящей из пяти частей, посвященных использованию услуг сторонних компаний с целью снижения риска кибербезопасности.

Если вы читаете это руководство, вы, вероятно, ознакомились с нашим **первым руководством** в этой серии - «Должен ли я получать внешнюю поддержку для управления рисками кибербезопасности?», и решили, что вам действительно следует искать какую-то форму поддержки извне. Ваш следующий вопрос мог бы звучать так: какие есть варианты, когда дело доходит до внешней поддержки? Чтобы ответить на этот вопрос, обратитесь к нашему **второму руководству** из этой серии - «Обзор видов поддержки в области ИТ и кибербезопасности».

Теперь, когда вы понимаете свои варианты, вы готовы узнать, как выбрать лучший из них для ваших конкретных потребностей. В этом руководстве мы предоставляем пошаговые инструкции о том, как выбрать правильный уровень внешней поддержки. Мы предлагаем вам сохранить, загрузить или распечатать это руководство и использовать его в качестве настраиваемого рабочего листа для вашего бизнеса.

Шаг 1. Расставьте приоритеты

Расставьте приоритеты для ваших систем и данных. Какие из них наиболее важны для вашего бизнеса? Каковы ваши «наиболее ценные активы»? Перечислите их ниже.

info@cyberreadinessinstitute.com

Шаг 2. Рассмотрите возможность найма консультанта

Задайте себе следующие вопросы о том, является ли дополнительная поддержка логичным шагом для вашего бизнеса.

Должен ли я соблюдать правила?

Да **Нет**

Взаимодействую ли я с информацией о сотрудниках, личной информацией клиента (PII) или защищенной медицинской информацией (PHI)?

Да **Нет**

Мой бизнес находится в штате, где действуют законы о конфиденциальности?

Да **Нет**

Полностью ли я информирован о требованиях и ожиданиях моих клиентов?

Да **Нет**

Принимаю ли я кредитные карты в качестве оплаты?

Да **Нет**

Являюсь ли я частью цепочки поставок критической инфраструктуры?

Да **Нет**

Если ответы на вышеперечисленные вопросы в основном «да», то вам, вероятно, будет полезен советник по информационной безопасности/кибер-консультанту/виртуальный директор по информационной безопасности (vCISO). Они могут предоставить дополнительную поддержку, чтобы помочь вам в процессе выбора внешней поддержки.
Если ответы на приведенные выше вопросы в основном «нет», возможно, вам не нужна посторонняя помощь в определении того, какие аутсорсинговые услуги необходимы. Если это так, мы рекомендуем вам пройти Программу киберподготовки и Программу сертификации киберлидеров, а затем переоценить свои потребности.

Шаг 3: Разграничьте роли

Есть сотни компаний и частных лиц, готовых оказать вам внешнюю поддержку. Знание того, как определить лучшую внешнюю компанию для решения ваших бизнес-задач, — непростая задача. Многие консультанты могут не иметь надлежащей подготовки и опыта, необходимых для удовлетворения ваших уникальных требований безопасности.
Для получения дополнительной информации о типах организаций поддержки, профессиональных полномочиях, которые помогают указать, что человек хорошо осведомлен, и типах организаций, с которыми вы можете столкнуться, пожалуйста, повторно прочитайте **второе руководство** в этой серии: «Обзор видов внешней поддержки в области ИТ и кибербезопасности».

Поставщик управляемых услуг (MSP)

Стоимость МСП может варьироваться от 75 до 200 долларов США в час. Некоторые взимают фиксированную плату, а не почасовую, а другие взимают плату в зависимости от количества компьютеров или людей.

Виртуальный директор по информационной безопасности (vCISO)

Количество необходимого времени и плата варьируются, но стоимость найма vCISO может быть всего несколько сотен долларов в неделю.

Шаг 4: Выберите киберкуратора

Киберкуратор создает культуру соблюдения безопасности и обеспечивает реализацию соответствующих мер безопасности при поддержке высшего руководства и vCISO. Киберкуратор — это связующее звено в вашей компании между MSP и vCISO, если вы наняли vCISO.

Шаг 5: Определите свои требования

В следующей таблице перечислены некоторые из наиболее распространенных требований и действий, с которыми вам может понадобиться помощь. Поскольку вы различаете MSP и vCISO, используйте флажки ниже, чтобы указать, какие элементы имеют отношение к вашему бизнесу.

Если у вас есть проблемы с пониманием терминов и понятий в правой колонке, вам следует обсудить их с вашим MSP или настоятельно рассмотреть вопрос о найме консультанта, который поможет вам.

MSP

☐ Настройка сети на объекте

☐ Настройка сети в офисе

☐ Настройка удаленной сети

☐ Настройка компьютеров для новых пользователей

☐ Настройка учетных записей электронной почты

☐ Установка и поддержка программного обеспечения для обнаружения угроз и реагирования на них на конечных точках (антивирус).

☐ Выполнение резервного копирования данных

☐ Тестирование резервных копий

☐ Установка многофакторной аутентификации

☐ Настройка VPN

☐ Установка и обслуживание/ исправление программного обеспечения

☐ Определение/внедрение облачных сервисов

☐ Предоставление службы поддержки

☐ Внедрение брандмауэров на вашей сетевой архитектуре

☐ Определение соответствующих правил конфиденциальности данных (например, GDPR, CCPA)

vCISO (директор по информационной безопасности)

☐ Оценка/сравнение предложений от MSP

☐ Создание плана реагирования на инциденты

☐ Мониторинг доступа, брандмауэра и других журналов и реагирование на аномалии

☐ Отслеживание попыток атаки

☐ Проведение тестов на проникновение в сеть

☐ Установление допустимого использования персональных устройств

☐ Установка пароля и других стандартов

☐ Обеспечение быстрого и правильного исправления систем

☐ Определение технических требований и спецификаций таких, как VPN, брандмауэр, другие меры безопасности (элементы управления), сетевая архитектура и/или облачные службы.

☐ Проведение анализа рисков поставщиков

☐ Обеспечение того, что компьютеры не могут быть адресованы за пределы сети.

☐ Поддержка руководства компании в формировании культуры киберготовности

☐ Определение влияния поставщиков облачных услуг на безопасность, предоставление стандартов

☐ Определение и внедрение методов управления доступом к системам и информации, чтобы авторизованные пользователи имели доступ к тому, что им нужно, и не более того.

☐ Согласование элементов управления с соблюдением соответствующих правил конфиденциальности данных

Если большинство ваших полей в левом столбце отмечены флажками, вам следует нанять MSP. Если большинство флажков в правом столбце отмечены флажками, вам следует нанять vCISO. Если ваши флажки были расставлены поровну в обоих столбцах, рассмотрите возможность найма обоих.

Цель этого руководства — помочь вам определить, как выбрать правильный уровень поддержки. Если вы сейчас столкнулись с потенциально запутанными договорами, обратите внимание на наше следующее руководство из этой серии: «Изучение и понимание договора».

Полный список руководств этой серии:

Следует ли мне обратиться за внешней поддержкой для управления рисками кибербезопасности?

Обзор видов внешней поддержки ИТ и кибербезопасности

Как выбрать правильный уровень внешней поддержки

(ДАННОЕ РУКОВОДСТВО)

Изучение и понимание договора

Ваши текущие обязанности по кибербезопасности

Соавторы

Особая благодарность

- Марку Пиллону, IT Ally
- Брайану Келли, EDUCAUSE
- Доун Янкилов, TALK
- Фэй Франси, Auto-ISAC
- Илен Кляйн, Cybercrime Support Network
- Джилл Токуда, CyberHawaii
- Джону Брику, DNG-ISAC
- Майклу Причарду, Netchex
- Тане Болден, AIAG
- Уолтеру Брану, ICC Guatemala
- Стэну Шталю, SecureTheVillage

Об Институте киберготовности

Институт киберготовности — это некоммерческая инициатива, объединяющая лидеров бизнеса из разных секторов и географических регионов для обмена ресурсами и знаниями, которые используются с целью разработки бесплатных инструментов кибербезопасности в малых и средних предприятиях (МСП). Изучите основы хорошей кибербезопасности с помощью нашего Стартового набора или создайте культуру киберготовности в своей организации с помощью самостоятельной онлайн-программы киберготовности. В наших руководствах по ресурсам для удаленной работы и гибридным рабочим местам вы найдете своевременные советы по решению современных киберпроблем. Чтобы узнать больше, посетите сайт **www.BeCyberReady.com**.