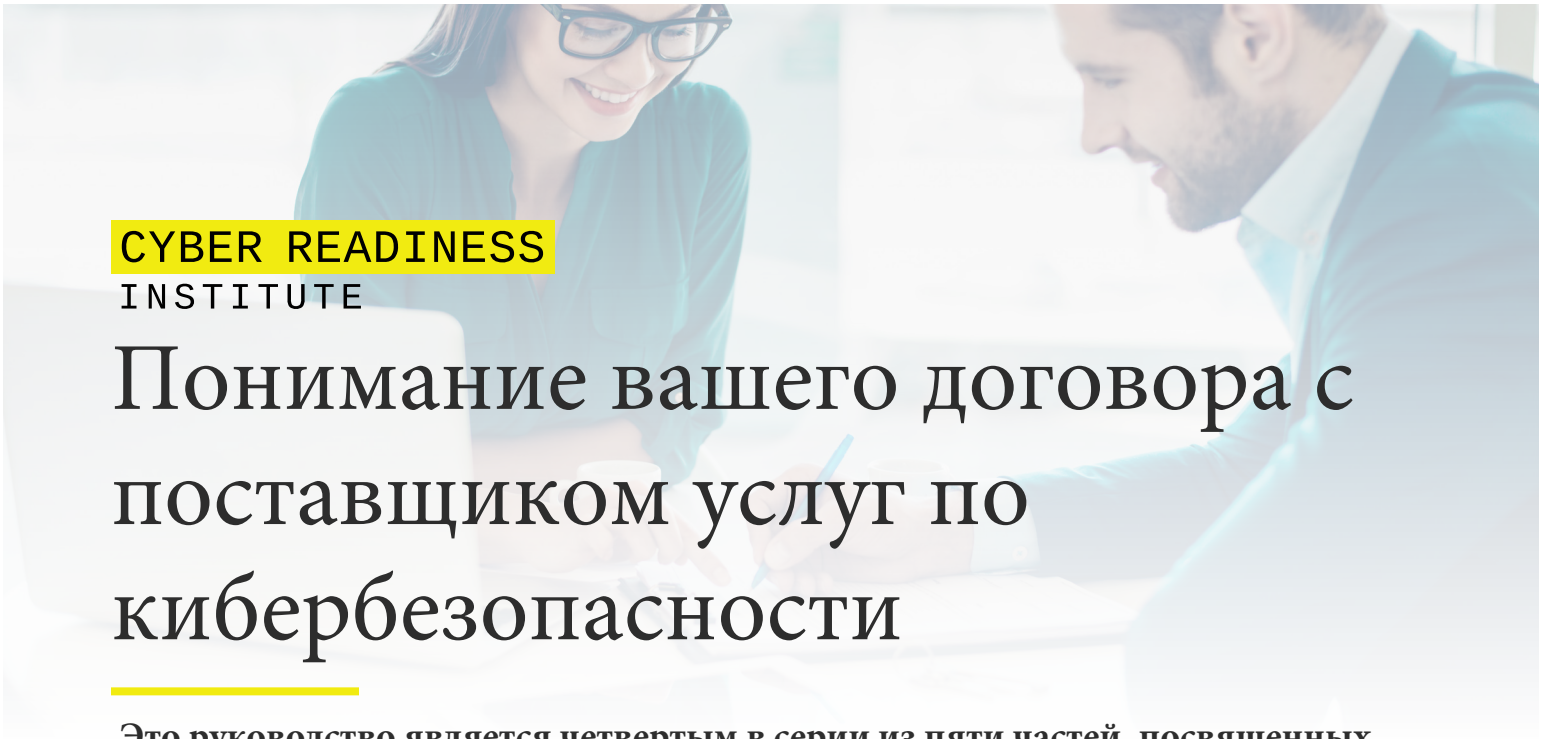

CYBER READINESS
INSTITUTE

Понимание вашего договора с поставщиком услуг по кибербезопасности

Это руководство является четвертым в серии из пяти частей, посвященных использованию услуг сторонних компаний с целью снижения риска кибербезопасности.

На этом этапе процесса вы решили заручиться внешней поддержкой для улучшения своей кибербезопасности. Мы предоставили вам руководство по различным видам поставщиков услуг и несколько советов по их оценке. В этом руководстве мы даем представление о том, на что вы (и/или ваш юрист) должны обратить внимание в договоре. Помимо юридических аспектов, договор является важнейшим документом, точно определяющим, какие именно услуги будут предоставляться, и вашими текущими обязанностями по обеспечению кибербезопасности.

Мы предлагаем вам использовать договор в качестве контрольного списка, чтобы убедиться, что у вас и вашего поставщика услуг есть взаимное понимание обязанностей в будущем. Вы должны убедиться, что все ваши ожидания оправдаются. Не попадайтесь в ловушку, ожидая атаки, чтобы понять, что входит в договор, и осознавая, что он не распространяется на то, что вам нужно.

Важно, чтобы вы установили доверительные отношения с вашим поставщиком услуг. В идеале он должен стать частью команды, помогающей вашей организации создавать и поддерживать функциональные и безопасные ИТ-возможности. Убедиться в том, что вы понимаете договор и обязанности поставщика, имеет решающее значение для установления доверия с самого начала. Кроме того, мы предлагаем вам проводить ежеквартальный аудит с поставщиком услуг, во время которого вы будете использовать договор в качестве контрольного списка для оценки отношений и того, как он служит вашей компании и ее потребностям. Угрозы кибербезопасности становятся более изощренными, и вы должны быть уверены, что вы и ваш поставщик услуг не только готовы реагировать, но и активно внедряете меры для того, чтобы оставаться защищенными и киберустойчивыми.

Мы разделили это руководство на три части: **Проверка до подписания договора, Контрольный список договора и Руководство по изучению договора.**

info@cyberreadinessinstitute.com

Проверка до подписания договора

Прежде чем приступить к подробному обсуждению договора, важно узнать о приоритетах, опыте и практике вашего потенциального поставщика услуг. Вот некоторые ключевые вопросы, которые следует изучить в отношении предлагаемого поставщика услуг ДО подписания договора. На следующие вопросы нет «правильных» ответов; они предназначены для того, чтобы помочь вам понять уровень сложности вашего поставщика услуг.

Вопросы к вашему поставщику услуг

1. Определите контактное(-ые) лицо(-а) у поставщика по конкретным услугам и укажите, кто будет вашим постоянным менеджером по работе с клиентами.
2. Убедитесь в том, что сотрудники поставщика услуг прошли соответствующие проверки безопасности (т. е. проверку биографических данных) при работе с конфиденциальной информацией.
3. Убедитесь, в том, что у вашего поставщика есть страховка от киберугроз, и проверьте степень/лимит покрытия на случай киберинцидентов в вашей компании. Это поможет вам определить возможные пробелы в покрытии между страховкой поставщика услуг и страховкой, которая у вас есть или которой у вас нет.
4. Спросите об их уровне контроля безопасности и о том, соответствуют ли они каким-либо стандартам или структурам (сертификаты или учетные данные такие, как NIST 800-53, NIST Cybersecurity Framework, ISO27001, FedRamp, и/или аудиторские отчеты такие, как SOC2).
5. Узнайте о часах службы поддержки (т. е. это обычные рабочие часы или круглосуточно и без выходных?). Доступен ли поставщик услуг «в нерабочее время»?
6. Если они размещают какое-либо программное обеспечение или данные, выясните, где они размещены и кто контролирует эти серверы, и попросите поставщика услуг уведомлять вас о любых изменениях. В некоторых случаях поставщик услуг может только оказывать вам поддержку, а не размещать какое-либо ваше программное обеспечение или данные.
7. Определите, пользуется ли поставщик услугами других компаний или субподрядчиков для предоставления вам услуг.
8. Спросите, не является ли поставщик услуг частью какой-либо организации или службы, которая может предоставлять информацию об угрозах.

Контрольный список договора

Ниже мы приводим некоторые рекомендации по оценке вашего договора с вашим поставщиком услуг по кибербезопасности. В следующей таблице мы предлагаем некоторые предложения по обязательным услугам, которые должны быть указаны в договоре, а также некоторые дополнительные элементы, которые следует учитывать.

Обязательно

☐ Доступность службы поддержки – доступные часы поддержки включены в базовый ценовой пакет.

☐ Документация и руководства пользователя для соответствующего оборудования и программного обеспечения

☐ Настройка оборудования (например, серверы, ноутбуки, Wi-Fi, смартфоны)

☐ Установка и обновление программного обеспечения

☐ Техническая поддержка сети

☐ Консалтинг (виртуальный ИТ-директор)

☐ Резервное копирование и восстановление (объем, тестирование, периодичность)

- **Резервные копии находятся в автономном режиме?**
- **Зашифрованы ли резервные копии?**

☐ Методы шифрования данных

- **Зашифрованы ли хранящиеся данные?**
- **Зашифрованы ли передаваемые данные?**

☐ Определение уровня приоритетного реагирования (примеры ниже)

- **ПРИОРИТЕТ 1 — в масштабах предприятия — с немедленным финансовым эффектом — менее 30 минут**
- **ПРИОРИТЕТ 2 — проблемы, связанные с конкретным отделом или приложением — от 30 минут до 4 часов.**
- **ПРИОРИТЕТ 3 – затронут один человек – от 4 до 8 часов**

☐ Пункт об эскалации с поставщиком услуг в случае нерешенных проблем

☐ Основные контактные лица службы реагирования на инциденты (продавец и покупатель)

☐ Минимальные требования к безопасности

- **Active Directory или аналогичная установка для контроля доступа**
- **Конфигурация сети • Сроки обновлений (например, поставщик исправит критические уязвимости в течение 1–3 рабочих дней).**
- **Поставщик уведомляет о нарушении безопасности в течение установленного периода времени.**
- **Целевой показатель хостинга и времени безотказной работы, который включает максимальное целевое время простоя**
- **Видимость того, где хранятся данные**
- **Процесс адаптации и расписание**

☐ Пункт о прекращении исполнения

Желательно

☐ **Сетевой и системный архитектор/администратор**

☐ **Консультационные услуги (не указанные в другом месте) и обмен передовым отраслевым опытом**

☐ **Поддержка пользователей для удаленных сотрудников**

☐ **Поддержка пользователей для сотрудников, использующих персональные устройства**

☐ **Поддержка в нерабочее время**

☐ **Покупательная способность (скидки на оборудование и программное обеспечение при оптовых закупках)**

☐ **Проверка журналов (частота)**

☐ **Частота и объем отчетов о сетевой активности**

☐ **Участие в проведении учений по киберреагированию, включая реагирование на инциденты и симуляционное обучение**

☐ **Обучение (тип и частота такие, как многофакторная аутентификация, VPN, безопасная передача данных и т. д.)**

☐ **Помощь в разработке плана реагирования на инциденты**

- **Ответственность и роли в инциденте**
- **Дополнительные расходы, связанные с инцидентом**

info@cyberreadinessinstitute.com

Руководство по изучению договора

Некоторые вопросы подлежат обсуждению, но вы должны убедиться в том, что знаете, каким должен быть поставщик услуг, и определить правильный вид поставщика, прежде чем заключать официальный договор. Если вам нужна помощь в выборе правильного вида поставщика услуг, обратитесь к предыдущим руководствам этой серии.

Ниже приведен отрывок из договора, в котором излагается общий подход поставщика к отношениям и услугам, которые они будут предоставлять. Не все поставщики услуг предоставляют так много подробностей о своем подходе, но вы можете использовать это в качестве **руководства для некоторых общих аспектов**, которые следует учитывать:

«Наша команда и Центр поддержки также осуществляют управление сетью, в том числе выступают в качестве координационного центра для всех потребностей управления договорами с поставщиками услуг. **Кроме того, мы предоставляем квалифицированную команду, инфраструктуру и ресурсы для проектирования и разработки веб-сайтов и программного обеспечения для таких проектов, как веб-сайты на основе баз данных**. [Поставщик удаленных услуг] обеспечивает упреждающий индивидуальный подход к решению проблем. Миссия [Поставщика удаленных услуг] включает в себя предоставление профессиональной, удобной для клиентов среды для **администрирования и поддержки системы на месте**. Мы достигаем своей миссии за счет правильного сочетания людей, процессов и технологий. Наш подход позволяет обеспечивать высочайший уровень обслуживания клиентов как с помощью нашего персонала на месте, так и удаленно через наш Центр поддержки. **Мы внедряем качественные технологии и настраиваемую документацию с конкретными бизнес-правилами, рабочими процессами и каталогами устройств/аксессуаров/тарифных планов, чтобы технологии могли соответствовать правилам.** Другие предлагаемые услуги: [Поставщик управляемых услуг] предоставляет альтернативы устранению неполадок и поддержке **крупных рабочих станций и серверов, беспроводным устройствам,** обеспечению достоверности информации, **шифрованию данных, защите от ограничения брандмауэра**, безопасным ИТ-соединениям, биометрии, управлению ИТ-проектами, **колл-центру,** управлению ИТ-ресурсами и поддержкой, **веб-наблюдению**».

На следующей странице приведена выдержка с конкретными положениями из договора. Обратите внимание на уровень детализации сроков оказания услуг и специфику ответственности клиента:

ПРИЛОЖЕНИЕ ТЗ № C1-2017-205-433

В соответствии с условиями Соглашения о предоставлении профессиональных услуг («Соглашение») Стороны заключают настоящее Техническое задание («ТЗ»).

Прекращение

1. Период исполнения. Первоначальный период исполнения будет с 1 ноября 2018 г. по 30 ноября 2019 г. Если Сторона не предоставит письменное уведомление о расторжении до окончания Исходного периода исполнения, Соглашение будет действовать на ежемесячной основе до тех пор, пока Сторона не направит письменное уведомление о расторжении в соответствии с Соглашением.

Стандартные часы работы службы поддержки

2. Услуги. Услуги будут предоставляться на месте или удаленно, как это определяется по единоличному усмотрению [Поставщика удаленных услуг], в первую очередь по местонахождению Клиента. Стандартная поддержка будет предоставляться с 9:00 до 18:00 по восточному поясному времени с понедельника по пятницу, за исключением государственных праздников, отмечаемых Клиентом. Экстренная поддержка в нерабочее время и мониторинг сети будут предоставляться круглосуточно, 7 дней в неделю, в течение всего года.

Скорость обслуживания

3. 2.1 Покрываемые услуги 2.1.1. **Служба поддержки**. [Поставщик удаленных услуг] предоставит систему продажи билетов (ConnectWise) и **инструмент управления удаленным мониторингом** (RMM) (N-able), а также антивирус (Sophos). Клиент отправит все вопросы через клиентский онлайн-портал, по электронной почте или по горячей линии. Клиент сможет получать электронную почту, телефон или удаленную поддержку, чтобы помочь решить любые проблемы с компьютером, которые могут снизить производительность. **В случае чрезвычайной ситуации на месте технический специалист [Поставщика удаленных услуг] подтвердит в течение 30 минут и прибудет на место в течение 2 часов**. Любое неэкстренное обслуживание на месте будет запланировано между [Поставщиком удаленных услуг] и Клиентом, но может быть запрошено [Поставщиком удаленных услуг] для **выполнения в течение 4 рабочих часов, если Клиент решит, что это необходимо для обеспечения ИТ-операций.** [Поставщик удаленных услуг] приедет на место к любому объекту Клиента в районе [города], и поездка НЕ будет оцениваться как дополнительная плата. [Поставщик удаленных услуг] будет управлять эл. почтой Клиента, обеспечивая управление конечными пользователями, добавляя или удаляя учетные записи эл. почты, профили пользователей и настройку компьютера. Клиент должен предоставить уведомление за 5 рабочих дней до создания или удаления нового пользователя. Клиент заполнит шаблон на клиентском портале, предоставленном [Поставщиком удаленных услуг] для новых пользователей и прекращения действия пользователей.

Это руководство было разработано с тем, чтобы помочь вам изучить и понять потенциальные договоры, прежде чем официально сотрудничать с поставщиком услуг. В нашем следующем и последнем руководстве из этой серии мы обсудим, как управлять текущими отношениями после того, как вы подписали договор. Помните, что цель договора — установить ожидания для построения доверительных отношений между вами и вашим поставщиком услуг.

Полный список руководств этой серии:

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

Обзор видов внешней поддержки ИТ и кибербезопасности

Как выбрать правильный уровень внешней поддержки

Изучение и понимание договора

(ДАННОЕ РУКОВОДСТВО)

Ваши текущие обязанности по кибербезопасности

Соавторы

Особая благодарность

- Марку Пиллону, IT Ally
- Брайау 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 Гватемала
- Стэн Шталь, SecureTheVillage
- Лизе Маколи,GTPA
- Синат Согал, Cyber Academy for Kids through Empowerment
- Кэти Шульц, SUNY Cobleskill
- Шону Филиповски, SUNY Cobleskill

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**.