Преимущества аутсорсинга услуг кибербезопасности: защита от угроз и оптимизация расходов

Содержание

Введение

В эпоху цифровизации данные становятся одним из основных активов и стратегических ресурсов как бизнеса, так и государства. Помимо хакерских преступных групп, целью которых является финансовая выгода, последние годы наблюдается значительно возросшая активность политически мотивированных проправительственных групп и хактивистов, заинтересованных проведении диверсий, шпионажа и уничтожения данных, что выводит вопросы кибербезопасности на передний план. Однако не каждая компания или ведомство может позволить себе содержать собственный штат экспертов по информационной безопасности. Именно поэтому аутсорсинг услуг кибербезопасности становится всё более популярным решением для организаций и ведомств любого масштаба. Давайте рассмотрим, какие преимущества получает организация, когда передает задачи по киберзащите на внешнее обслуживание.

Снижение затрат и оптимизация ресурсов

Одним из ключевых аргументов в пользу аутсорсинга кибербезопасности является значительное снижение расходов. Формирование собственного отдела безопасности требует серьезных инвестиций в:

- набор и обучение сотрудников;
- закупку оборудования, программного обеспечения и технической поддержки;
- постоянное обновление решений и технологий.

позволяет компаниям избежать расходов, связанных с простоем или восстановлением после кибератак, минимизируя риски благодаря своевременному реагированию на угрозы.

Доступ к передовым технологиям и профессиональному опыту

Одним из важнейших преимуществ аутсорсинга является возможность доступа к экспертным знаниям и передовым технологиям. Поставщики услуг кибербезопасности обладают обширным опытом работы с разными типами угроз, что позволяет им своевременно реагировать на инциденты.

Экспертиза в различных областях
Специалисты аутсорсинговых компаний регулярно обучаются и проходят сертификацию по новейшим стандартам безопасности. Внутренний штат специалистов, особенно в небольших компаниях, зачастую ограничен в возможностях следить за всеми аспектами защиты и изменениями в законодательстве. В то время как аутсорсинговые компании предлагают:

- глубокие знания в узкоспециализированных областях, таких как обеспечение безопасности веб-приложений, управление и расследование инцидентов;
- доступ к аналитическим данным по актуальным угрозам и новейшим уязвимостям;
- использование передовых технологий для мониторинга и обнаружения угроз в режиме реального времени.

Использование лучших практик
Профессиональные компании по кибербезопасности, предоставляющие аутсорсинг, часто работают по лучшим мировым стандартам и придерживаются передовых практик. Это включает внедрение международных стандартов, таких как ISO 27001, и регулярное тестирование систем на уязвимости, что позволяет клиентам быть уверенными в качестве защиты.

Круглосуточный мониторинг и оперативное реагирование

Кибератаки происходят в любое время, и без постоянного мониторинга даже кратковременный сбой в системе безопасности может привести к катастрофическим последствиям. Организации и ведомства часто ограничены в ресурсах, чтобы обеспечить круглосуточный контроль за всеми процессами, тогда как аутсорсинг позволяет получить полноценный мониторинг и поддержку в режиме 24/7.

Проактивный подход к защите
Аутсорсинговые компании внедряют проактивные подходы к киберзащите, которые включают:

- мониторинг сетевой активности в реальном времени;
- предупреждение о потенциальных угрозах до того, как они могут нанести ущерб;
- оперативное реагирование на инциденты и устранение уязвимостей.

Быстрое восстановление после инцидентов
В случае обнаружения инцидента, аутсорсинговая компания может быстрее организовать ответные меры благодаря отлаженным процессам и опыту. Это минимизирует последствия для бизнеса и сокращает время простоя. Для некоторых компаний это может стать критическим фактором выживания на рынке, особенно если речь идет о финансовом секторе или электронных услугах.

Масштабируемость и гибкость

Аутсорсинг услуг по кибербезопасности дает компаниям возможность гибко управлять своими ресурсами в зависимости от текущих потребностей. Внутренние решения часто фиксированы и не поддаются быстрой адаптации, что может создать сложности при росте бизнеса или изменении инфраструктуры.

Подстраивание под нужды бизнеса
Аутсорсинговые компании предлагают гибкие тарифные планы и могут адаптировать свои услуги под конкретные задачи:

- набор услуг можно изменять в зависимости от того, насколько сложна инфраструктура компании или какие требования безопасности актуальны в данный момент;
- компании могут увеличивать или уменьшать объемы услуг в зависимости от сезонных или рыночных факторов без необходимости кардинальной перестройки собственной инфраструктуры.

Снижение риска и соответствие нормативным требованиям

Современные нормативные акты требуют от компаний выполнения определенных стандартов безопасности и защиты данных. Несоответствие этим требованиям может привести к юридическим последствиям и крупным штрафам. Передача задач по обеспечению кибербезопасности внешним профессионалам позволяет снизить эти риски.

Комплаенс и аудит
Поставщики услуг по кибербезопасности обеспечивают выполнение всех

требований комплаенса, помогая компаниям соблюдать местные и международные законы, например, ФЗ-152 (О защите персональных данных), ФЗ-187 (О безопасности критической информационной инфраструктуры Российской Федерации) или GDPR (Общий регламент по защите данных). Компании специализирующиеся на кибербезопасности регулярно проводят аудиты на соответствие стандартам безопасности, участвуют в программах bug-bounty и могут предоставить отчетность для регулирующих органов. Это снижает риск нарушения законодательства и потенциальных санкций со стороны органов надзора.

Страхование рисков
Многие аутсорсинговые компании предлагают дополнительные услуги, такие как страхование киберрисков. Это обеспечивает дополнительную защиту на случай непредвиденных инцидентов, которые могут привести к утечке данных или нарушению работы.

Фокус на основной деятельности

В современном бизнесе кибербезопасность становится всё более сложной задачей, требующей постоянного контроля и анализа. Для многих компаний управление безопасностью отвлекает от основной деятельности, особенно если их бизнес не связан с информационными технологиями. Аутсорсинг позволяет передать эту сложную и трудоемкую задачу на внешнее управление, освобождая ресурсы для стратегического развития компании.

Улучшение производительности
Передача задач по обеспечению кибербезопасности стороннему подрядчику позволяет:

- сконцентрироваться на ключевых аспектах бизнеса, таких как разработка продуктов, маркетинг и продажи или же государственном управлении;
- обеспечить непрерывность бизнес-процессов, не беспокоясь о рисках кибератак.

Это повышает общую производительность и эффективность, позволяя избежать простоев и сбоев, вызванных внутренними инцидентами безопасности.

Долгосрочная стратегия киберзащиты

Одним из ключевых факторов успеха аутсорсинга кибербезопасности является возможность разработки долгосрочной стратегии защиты. Внешние поставщики могут предложить компаниям:

- стратегические планы по улучшению и усилению защиты;
- постоянный мониторинг изменений в сфере безопасности и адаптацию к новым угрозам.

Заключение

Аутсорсинг услуг по кибербезопасности представляет собой важное стратегическое решение для организаций и ведомств, стремящихся обеспечить защиту как своих, так и вверенных им данных, сократить затраты и повысить эффективность. Он позволяет получить доступ к экспертным знаниям, передовым технологиям и круглосуточному мониторингу, что несомненно делает его привлекательным вариантом для бизнеса и государственных структур любого размера.

Чем мы можем Вам помочь?

ООО «НТЦ ЕВРААС», являясь многопрофильной коммерческой структурой, имеет все необходимые лицензии регуляторов рынка информационной безопасности, в том числе лицензии на осуществление работ с использованием сведений, составляющих государственную тайну.

Обладая фундаментальными знаниями и опытом в области защиты информации, эксперты НТЦ «ЕВРААС» предлагают новейшие комплексные разработки в сфере обеспечения безопасности компаний розничной торговли.

Мы проектируем системы под конкретные нужды и специфику организаций, тем самым гарантируя, что система информационной безопасности комплексно решает все задачи и обеспечивает надежную круглосуточную защиту ваших корпоративных ресурсов и данных.

Контакты:

г. Москва, ул. Автозаводская 13/1

8 (495) 748-09-44

evraas@evraas.ru