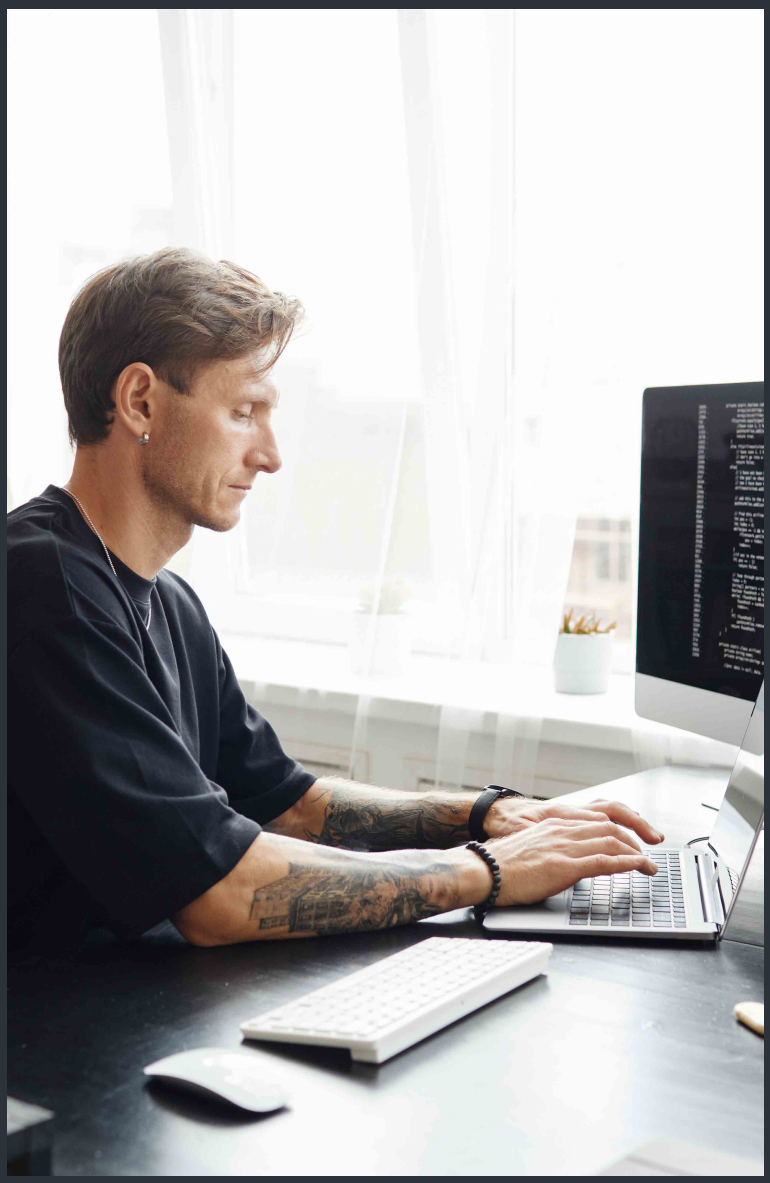
# КАК БОРОТЬСЯ С SHADOW IT, ИЛИ ВЫХОДИМ ИЗ ТЕНИ С ПОМОЩЬЮ ШЛЮЗА ВЕБ-БЕЗОПАСНОСТИ



## РУКОВОДСТВО ДЛЯ КРУПНЫХ ОРГАНИЗАЦИЙ

Использование сотрудниками не разрешенного к применению ПО повышает риск утечки ценной корпоративной информации. Пренебрежительное отношение к информационной безопасности в целом может обернуться для компании финансовыми и репутационными потерями.

Мы подготовили материал, в котором расскажем, в чем опасность теневых ИТ (Shadow IT) и почему шлюз веб-безопасности можно использовать для решения этой проблемы.

ТЕНЕВЫЕ ИТ — ЭТО ВСЕ ПРОГРАММЫ, ОБЛАЧНЫЕ СЕРВИСЫ И АППАРАТНЫЕ РЕШЕНИЯ, НЕ ОДОБРЕННЫЕ К ПРИМЕНЕНИЮ СЛУЖБАМИ ИТ ИЛИ ИБ КОМПАНИЙ. С ПЕРЕХОДОМ МНОГИХ СОТРУДНИКОВ НА УДАЛЕННУЮ РАБОТУ ИХ ИСПОЛЬЗОВАНИЕ СОЗДАЕТ КРУПНОМУ БИЗНЕСУ СЕРЬЕЗНЫЕ ПРОБЛЕМЫ, РЕШЕНИЕ КОТОРЫХ ПОЗВОЛИЛО БЫ ИЗБАВИТЬСЯ ОТ ФИНАНСОВЫХ РИСКОВ, ПРОБЛЕМ С ЗАКОНОМ И УГРОЗ БЕЗОПАСНОСТИ.

85%

сотрудников регулярно или периодически используют теневые ИТ

65%

сотрудников, работающих на удаленке, регулярно используют теневые ИТ

58%

менеджеров среднего и высшего звена используют теневые ИТ

42%

сотрудников пользуются сторонними почтовыми сервисами

38%

сотрудников пользуются сторонними мессенджерами

35%

сотрудников пользуются сторонним ПО для видеоконференций

28%

сотрудников пользуются сторонними платформами для совместной работы

## ПРАВОВЫЕ РИСКИ

Не согласованное с ИБ-службой ПО, устанавливаемое на рабочие компьютеры сотрудниками российских компаний, — преимущественно европейского и американского происхождения. Его использование противоречит требованиям указов и распоряжений Правительства и Президента РФ о необходимости импортозамещения продуктов в сфере информационных технологий. Несмотря на то что правоприменительная практика по данным нормативным актам только формируется, тем не менее можно ожидать, что контроль за их соблюдением будет достаточно жестким и санкции в отношении компаний-нарушителей будут значительно влиять на их операционную деятельность.

## ГЛАВНЫЕ АСПЕКТЫ ПРОБЛЕМЫ

01 Повышение риска утечки личных данных клиентов и, как следствие, санкции, предусмотренные Федеральным законом «О персональных данных» от 27 июня 2006 г. № 152-ФЗ.

02 Использование в компании теневого, нелицензированного ПО в коммерческих целях возлагает на сотрудников и руководство административную и уголовную ответственность в соответствии со ст. 7.12 КоАП РФ и ст. 146 УК РФ.

## ФИНАНСОВЫЕ РИСКИ

С одной стороны, сотрудники и целые подразделения покупают доступы к продуктам, не одобренным департаментом ИБ. При этом часто за счет не предназначенных для этих целей статей бюджета. В свою очередь нецелевое расходование средств затрудняет финансовый контроль, бюджетное планирование и отчетность.

С другой стороны, компания приобретает одобренное департаментом ИБ лицензированное ПО, которое по факту не используется. Отсутствие учета такого ПО приводит к тому, что лицензии продолжают закупаться не всегда с пользой для дела. Предотвратить финансовые потери в этом случае достаточно сложно, поскольку трудно их оценить.

## РИСКИ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

### НАЛИЧИЕ УЯЗВИМОСТЕЙ В ПО

Если программное обеспечение используется в обход ИТ/ИБ-службы, то оно не проверяется на предмет наличия в нем подозрительного кода и его использование может поставить под угрозу целостность ИТ-инфраструктуры и привести к серьезным инцидентам безопасности.

### УТЕЧКА ДАННЫХ ЧЕРЕЗ ОБЛАЧНЫЕ СЕРВИСЫ

Большинство утечек происходит через облачные сервисы. Если эти сервисы не контролируются, то легко допустить случайную утечку или намеренную передачу конфиденциальной информации.

# КАК С ПОМОЩЬЮ ШЛЮЗА ВЕБ-БЕЗОПАСНОСТИ ЗАЩИТИТЬ КОМПАНИЮ ОТ УГРОЗ, ИСХОДЯЩИХ ОТ ТЕНЕВЫХ ИТ

## ПРОВЕДИТЕ ИНВЕНТАРИЗАЦИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И КАТЕГОРИЗАЦИЮ ВЕБ-РЕСУРСОВ

Это самый важный шаг в борьбе с Shadow IT, ведь основной причиной является именно непонимание масштаба используемого в компании программного обеспечения и отсутствие контроля над ним и посещаемыми сайтами или сервисами. Чтобы получить полную информацию о киберландшафте, используйте решения с агентами для рабочих станций, которые способны выгрузить информацию по установленным у пользователей программам. Такими решениями могут быть антивирусы, DLP и другие системы для крупного бизнеса. Если на предприятии установлены отдельные системы для инвентаризации и учета активов с возможностью сбора данных с рабочих станций — их тоже можно использовать.

Чтобы получить недостающую информацию об облачных сервисах и продуктах, доступ к которым осуществляется через интернет, удобнее всего использовать программное обеспечение с категоризацией веб-ресурсов, не входящих в белый список. Результаты анализа трафика с помощью шлюза веб-безопасности с «умным» категоризатором, созданным с помощью технологии искусственного интеллекта, позволят в будущем принять решение о блокировке именно тех нежелательных сайтов, которыми пользуются сотрудники.

В этом случае не придется тратить средства на хранение в системе неработающих правил или добавление в черный список веб-страниц вручную.

## ОБНОВИТЕ МОДЕЛЬ УГРОЗ И ПОЛИТИКУ ИБ

Оцените риски, связанные с использованием в вашей организации тех или иных программ или веб-ресурсов, и с учетом этих данных обновите модель угроз. Посмотрите, как выглядит текущая ролевая модель предоставления доступа и есть ли смысл обновить и ее. Особенно это актуально в случае, если количество теневых веб-ресурсов значительно, и реализация этих мер поможет создать действительно работающую модель угроз и политику безопасности. Внедрите обновленные элементы политики, обращая внимание на следующие методы обеспечения безопасности:

### ОРГАНИЗАЦИОННЫЕ МЕТОДЫ

Практикуйте подход, при котором человек рассматривается как источник угрозы. Часто люди используют не одобренное к применению и даже запрещенное ПО из-за неудобства его инструментария или незнания, что в компании ему есть альтернативы, а вовсе не из-за желания навредить. Своевременное информирование и обучение пользователей — одна из важнейших составляющих успеха борьбы с Shadow IT.

### ПРОГРАММНЫЕ МЕТОДЫ

Предложение установить альтернативные программы взамен удаления «серых» и блокировка доступа к веб-ресурсам или конкретным страницам на сайте (например, для блокировки оплаты сервиса) кажется оптимальным вариантом при реализации обновленной политики безопасности. Рекомендуется подготовить сотрудников к такому переходу: взаимодействуйте при этом с HR-департаментом и отделами, отвечающими за ИТ-процессы, собирайте обратную связь от пользователей и устанавливайте гибкие правила ролевого разграничения доступа.

ВАЖНО ПОМНИТЬ: чтобы избежать рисков, связанных с нарушением процессов производства продуктов или услуг, следует обеспечить информационную безопасность компании в качестве залога долгосрочной устойчивости бизнеса, поэтому борьба с такой сложной и многогранной проблемой, как теневые ИТ, не должна быть в этом смысле исключением.




SOLAR БЕЗОПАСНОСТЬ ЗА НАМИ

T +7 (499) 755-07-70
E info@rt-solar.ru

Центральный офис, 125009, Москва
Никитский переулок, 7с1