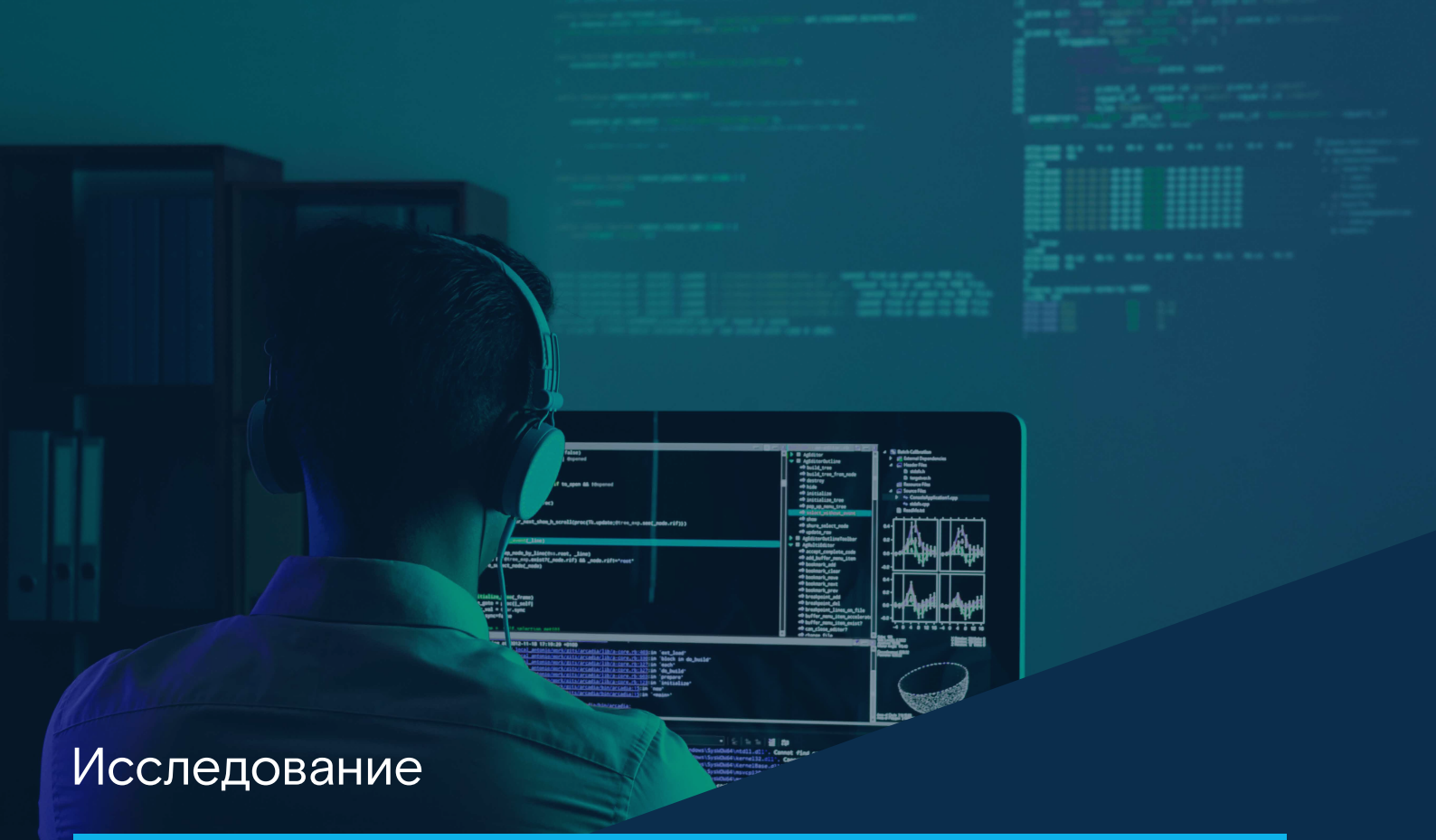


Исследование

Контроль конфиденциальной информации: аутсорсинг или in-house?

rt-solar.ru
solar@rt-solar.ru

Ростелеком
Солар

Оглавление

Ключевые цифры 03

Методология 04

Введение 05

Результаты исследования 06

- Разновидности и распространенность аутсорсинговой модели 06
- География аутсорсинга 07
- Риски аутсорсинга 07
- Риски самостоятельного использования DLP 08
- Цена аутсорсинга 09

Выводы 10

Контакты 10

Ключевые цифры

52% респондентов эксплуатируют DLP-систему самостоятельно

11% из них считают оптимальным частичный аутсорсинг

16% респондентов, эксплуатирующих DLP самостоятельно, опасаются возможной концентрации неограниченной власти у сотрудников, имеющих доступ к информации о коллегах

18% респондентов используют DLP-систему частично или полностью в аутсорсинговой модели

23% респондентов пользуются полным аутсорсингом

23% респондентов, использующих частичный аутсорсинг, представляют регионы

- 76% опрошенных считают, что наибольший риск аутсорсинговой модели – утечка информации об утечках
- 17% опрошенных считают, что второй по критичности риск – снижение скорости реагирования на инциденты

- 75% респондентов считают, что стоимость аутсорсинговой модели должна определяться масштабами возможного ущерба
- 21% респондентов называют усредненную фиксированную стоимость в границах от 1 до 10 млн рублей за инсталляцию DLP-системы на рабочие станции 1000 сотрудников

Методология

В процессе опроса респондентам предлагалось выбрать один из предложенных вариантов ответов или указать свой вариант ответа в свободной форме.

Данное исследование проведено методом электронного опроса специалистов по информационной безопасности – посетителей сайта компании «Ростелеком-Солар», интернет-портала информационно-аналитического центра Anti-Malware.ru, а также интернет-ресурса по информационной безопасности Securitylab.ru.

В опросе приняли участие представители российских организаций, относящихся к сегментам среднего и крупного бизнеса.

Опрос проводился в период с апреля по май 2022 года.

>200 респондентов приняли участие в исследовании

Введение

Компания «РТК-Солар», национальный провайдер технологий и сервисов кибербезопасности, представляет исследование «Контроль конфиденциальной информации: аутсорсинг или in-house?».

Тематика исследования выбрана неслучайно: концепция кибербезопасности (в том числе и для защиты от внутренних угроз) как сервиса стремительно набирает популярность в последнее время. Однако многие организации все еще считают эту модель слишком рискованной. Одни боятся отдавать экспертизу и чувствительную информацию вовне, другие – не верят в компетенции исполнителей, третьи – ждут массового распространения соответствующей практики.

При этом разговоры о том, чтобы отдавать на аутсорсинг функции по контролю конфиденциальной информации, возникли практически одновременно с появлением DLP-систем как класса ИБ-продуктов. Эта тема остается в повестке диалога заказчиков и производителей DLP-систем более 10 лет. При этом похоже, что концепция такого диалога претерпевает постепенные изменения.

«Аутсорсинг ИБ? – Нет! Аутсорсинг DLP? – Точно нет!» – такова была краткая позиция любого заказчика ИБ-услуг в 2010–2012 гг. Однако со временем, с распространением аутсорсинговых моделей в самых разных форматах (например, облачное хранение почтовых архивов), передача внешним провайдерам функций обработки чувствительной информации перестает быть чем-то вызывающе тревожным. Или нет? Разбирались вместе с участниками исследования.

Результаты исследования будут полезны специалистам по информационной безопасности российских компаний, руководителям – при принятии решения о модели использования систем контроля конфиденциальной информации, а также широкому кругу читателей, интересующихся тематикой утечки данных.

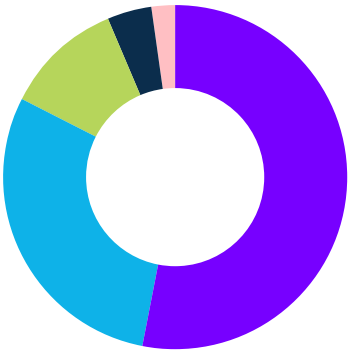
Результаты исследования

Разновидности и распространенность аутсорсинговой модели

52%

участников исследования в настоящее время эксплуатируют DLP-систему полностью самостоятельно.

В какой модели используется DLP?



52,1%
Система целиком эксплуатируется нами самостоятельно

29,6%
У нас в организации не используется DLP

11,3%
Гибридная: аналитическая работа с системой своими силами, техническое обслуживание – аутсорсинг

4,2%
Чистый сервис (услуги по эксплуатации системы и аналитическая работа в системе – целиком на аутсорсинге)

2,8%
Гибридная: техническое обслуживание своими силами, аналитическая работа с системой – аутсорсинг

11% респондентов считают оптимальным гибридный режим эксплуатации. При этом доля пользователей DLP-услуг в чисто сервисной модели (полный аутсорсинг: и техническая поддержка, и аналитическое сопровождение) невысока, **всего 4%.**

Данные исследования говорят о том, что заказчиков почти в 4 раза больше волнует конфиденциальность собираемой информации, чем доступ сторонних лиц к техническим средствам DLP-системы: техническую поддержку на аутсорсинг отдают в 4 раза чаще, чем привлекают внешних аналитиков для работы с внутренним, чувствительным трафиком.

В целом в том или ином формате (полный/частичный аутсорсинг) сервисную модель защиты от внутренних утечек называют оптимальной **21% участников** исследования. Характерно, что **40%** из них представляют сегмент крупного бизнеса: организации с численностью сотрудников свыше 1000 человек.

При этом, отвечая на вопрос «В каком случае организация может безопасно отдать услуги по контролю конфиденциальной информации на аутсорсинг?», **30% респондентов** называют отсутствие необходимых компетенций внутри организации. Этот вывод подтверждает отраслевая структура исследования: доля ИТ-компаний, самостоятельно эксплуатирующих DLP-систему, составляет 85%. При том что для других отраслей (среди которых здравоохранение, ТЭК, производство, ретейл и др.) средний процент самостоятельно эксплуатирующих DLP – **66%.**

Этот вывод полностью подтверждают результаты ответов на вопрос «В чем заключается наибольший риск аутсорсинговой модели?». 76% респондентов таким риском называют «Утечку информации об утечках». Конфиденциальная информация – дело сугубо внутреннее
и деликатное.

Основной вывод

Аутсорсинговая модель защиты от внутренних угроз – уже свершившийся факт, в том числе среди крупных организаций. Также приверженцы аутсорсинга есть даже среди тех заказчиков, которые в настоящее время эксплуатируют DLP-систему самостоятельно. При этом, судя по всему, основной фактор, блокирующий полную передачу сторонним подрядчикам в эксплуатацию систем контроля конфиденциальной информации, – это опасения, связанные с доступом к этой информации третьих лиц: аутсорсинговых аналитиков.

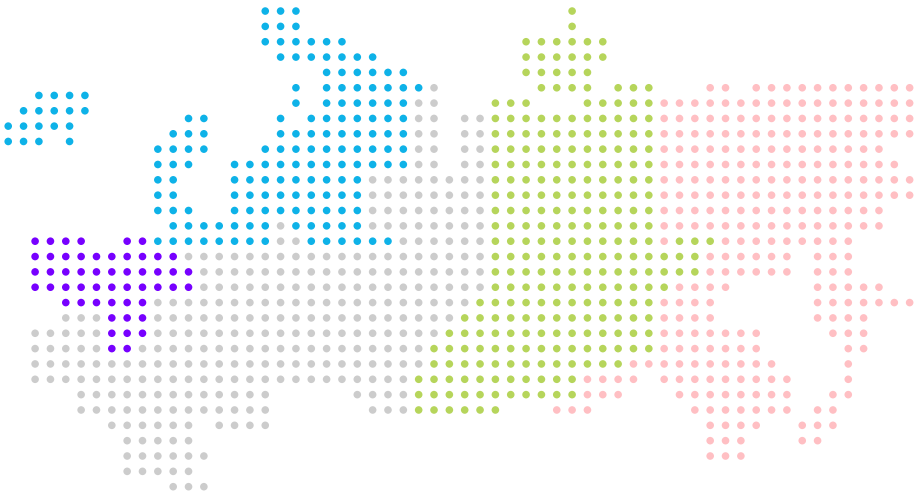
География аутсорсинга

77% Москва

7,7% Северо-Запад

7,7% ДВО

7,6% Урал



77%

респондентов, применяющих системы контроля конфиденциальной информации с помощью сторонних подрядчиков, представляют Москву, а 23% респондентов представляют другие регионы.

Основной вывод

> Доверие к внешним участникам такого деликатного процесса – явление достаточно распространенное и напрямую не зависит от региона.

Риски аутсорсинга

Наибольшим риском аутсорсинговой модели подавляющее большинство респондентов (76%) считает возможность утечки информации об утечках. Еще 17% считают таковым снижение скорости реагирования на инциденты.

Стоимость услуг аутсорсинга волнует всего чуть менее 3% респондентов. Тем не менее 13% из них считают подтвержденный опыт сервисной компании и его репутацию на рынке достаточными основаниями для безопасной передачи функций по контролю конфиденциальной информации на аутсорсинг.

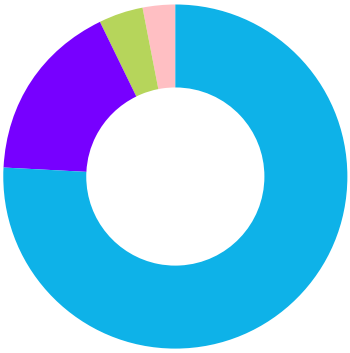
В чем риск аутсорсинга DLP?

76,1%
В утечках информации об утечках. Крнфиденциальная информация - дело сугубо внутреннее

16,9%
В снижении оперативности реагирования организации на инциденты

2,8%
В стоимости услуг

4,2%
Другое



Риски самостоятельного использования DLP

70%

Свыше 70% респондентов видят основной риск от самостоятельной эксплуатации DLP-систем организациями в недостаточности компетенций или ресурсов внутри организаций.

В чем наибольший риск самостоятельной эксплуатации DLP в организации?

56,3%

Недостаточность компетенций или ресурсов внутри организации приведет к неэффективному использованию DLP-системы, а значит, к утечкам конфиденциальной информации

16,9%

Учить безопасников долго и дорого. Это усугубляется рисками потери кадров такой квалификации, обладающих доступом к самой чувствительной информации в организации

15,5%

Если доступ к чувствительной информации есть у человека внутри организации, всегда есть риск, что он использует ее для собственной выгоды

11,3%

Другое

Очевидно, что эта проблема усугубилась в последнее время в связи с нарастающим объективным дефицитом кадров в сферах ИТ и ИБ. При этом значительная часть респондентов **(почти 16%)** опасается возможной концентрации неограниченной власти у сотрудников, имеющих доступ к информации о коллегах.

Цена аутсорсинга

Почти 75% респондентов считают, что стоимость аутсорсинговой модели должна быть гибкой и определяться масштабами возможного ущерба. Еще **21%** респондентов называют усредненную фиксированную стоимость в границах от 1 до 10 млн рублей за инсталляцию на рабочие станции 1000 сотрудников.

Какова оптимальная стоимость DLP-аутсорсинга?

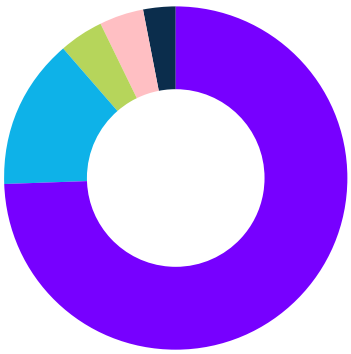
74,7%
Зависит от масштабов возможного ущерба, должна определяться условиями заказчика

14,1%
5 млн. руб.

4,2%
10 млн. руб.

4,2%
Не готовы вкладываться в аутсорсинг DLP

2,8%
1 млн. руб.



А теперь проведем сравнение за и против аутсорсинга по экономическим параметрам. Так, ориентировочная стоимость полного аутсорсинга (аналитическое и техническое сопровождение) DLP-системы с инсталляцией на 500–1000 рабочих станций сотрудников составляет 1,8–4 млн рублей. Окончательная цена зависит от объема делегированных заказчиком задач и SLA. Теперь попробуем оценить стоимость самостоятельной эксплуатации.

Средняя зарплата аналитика с опытом работы от 1 года составляет 130 000 рублей в месяц (данные рассчитаны на основании заработных плат, указанных работодателями на сайте hh.ru). Нужно понимать, что данный работник нанимается в первую очередь для сопровождения DLP-системы и работы по аналитике, настройке политик и расследованиям. Все вышеперечисленные обязанности будут занимать не менее 80% его рабочего времени. Кроме того, ему нужна замена на период отпуска, болезни и т. д.

Оклад инженера составит не менее 100 000 рублей в месяц при нагрузке по сопровождению DLP-системы не менее 50–60%. А для стабильной работы системы также потребуется второй инженер. Таким образом, ФОТ четырех специалистов без учета премий составит 5,5 млн руб. в год. Еще прибавьте к этому взносы в фонды, накладные расходы и затраты на повышение квалификации / переподготовку.

Можно пересчитывать плановые затраты на сопровождение DLP-системы исходя из объема выполняемых работ или за счет найма менее опытных специалистов. Выбор всегда остается за заказчиком.

Выводы

Подводя результаты исследования, аналитики компании «РТК-Солар» пришли к выводу, что время аутсорсинга защиты от утечек наконец настает. Все больше и больше компаний если еще не переходят на использование DLP как сервиса, то, по крайней мере, уже задумываются об этом и считают такую модель предпочтительной. Так, среди всех компаний-участников исследования, которые используют системы защиты от утечек, доля тех, кто делает это в форме частичного или полного аутсорсинга, составляет 26%. А также 11% тех, кто эксплуатирует DLP самостоятельно, считают, что лучше было бы использовать сервисную модель.

Эксперты «РТК-Солар» прогнозируют поступательный рост востребованности DLP-аутсорсинга в ближайшие годы. Этому способствуюти внешнеполитические и экономические реалии современной России, и внутренние процессы в отечественной отрасли ИБ. Конечно, для масштабного проникновения сервисной модели использования DLP рынку надо будет решить ряд важных задач. Необходимо правильно определить пул процессов и данных, которые можно отдавать на аутсорсинг, обозначить риски, закрепить ответственность сервис-провайдера за утечки данных, чтобы минимизировать возможные штрафы в адрес заказчиков.

Все это – вполне решаемые задачи.

Ростелеком
Солар

rt-solar.ru
rt.ru

Email:

solar@rt-solar.ru
support@rt-solar.ru

Телефоны:

+7 (499) 755-07-70 - продажи и общие вопросы
+7 (499) 755-02-20 - техническая поддержка

Адреса

125009, Москва, Никитский пер., 7, стр. 1
127015, Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд