

Развитие DLP-систем, как факторы повышения экономической безопасности бизнеса

Научный руководитель – Абрашкин Михаил Сергеевич

Петряев Владимир Сергеевич

Студент (бакалавр)

Технологический университет, Королёв, Россия

E-mail: vladimir-pv@outlook.com

Научно-технический прогресс не стоит на месте. С каждым годом рынок сфер информационной и экономической безопасности пополняется новыми решениями. Однако, компании ежегодно несут колоссальные убытки из-за утечек конфиденциальной информации, что является главной угрозой для экономической безопасности бизнеса.

По данным Infowatch, в России за 2019 год в сеть утекло более 172 млн записей пользовательских данных [1], что в 6 раз превышает показатели за 2018 год. При этом в 76% утечек виноваты сотрудники компаний. Чтобы решить данную проблему, были разработаны DLP- системы.

Такие системы создают защищенную цифровую «оболочку» вокруг сети устройств организации, анализируя всю входящую и исходящую информацию. Под контроль попадает не только интернет-трафик, но и ряд других информационных потоков: документы, выносимые за пределы защитной оболочки безопасности на внешних носителях, отправляемые на мобильные носители через Bluetooth, распечатываемые на принтере, передаваемые по другим потокам. Так же в задачи системы входит классификация конфиденциальности документов, перехваченных в трафике. Помимо этого, некоторые решения на DLP рынке ряд «побочных» функций. К ним следует отнести:

- 1) Контроль использования рабочего времени сотрудников.
- 2) Мониторинг общения сотрудников.
- 3) Контроль правомерности действий сотрудников.

Таким образом установка DLP-систем должна предотвращать большинство утечек, однако сегодня в России их использует лишь треть компаний [2]. И на это есть несколько причин. По данным исследования ScurityLab.ru [3], пользователи DLP выделяют следующие проблемы:

- 1) Отсутствие заявленного функционала рыночных решений (65%).
- 2) Технические проблемы, связанные с неправильным определением степени конфиденциальности данных (34%).
- 3) Сложность внедрения (35%).
- 4) Нехватка функционала (53%).
- 5) Отсутствие общей концепции работы с DLP (29%).

Выходит, что на сегодняшний день мы имеем неразвитую технологию, которая может существенно сократить утечку данных, и пользователей, которые, из-за малого количества решений на рынке и незнания концепции технологии, не используют DLP-системы. И

решить эти проблемы можно путем развития технологии. Чем больше развиваются DLP-системы, тем больше решений появляется на рынке. В условиях конкуренции, компании, поставляющие продукт, будут улучшать его, тем самым делая его более качественным и удобным для пользователя. Когда появятся качественные решения, пользователи начнут внедрять DLP-системы в своих компаниях, предотвращая утечки конфиденциальной информации и повышая экономическую безопасность бизнеса.

DLP-системы относительно новая технология, которая показывает высокие темпы роста ежегодно. Это не удивительно, ведь данная технология в обозримом будущем способна устранить человеческий фактор, как угрозу стабильности бизнеса. Каждый год мы видим новые решения на рынке антивирусов, шифрования и защит от атак. Мы все сильнее защищаем техническую часть, но забываем про самое слабое звено любой системы защиты: человека. Даже несмотря на то, что крупные организации проводят тренинги для своих сотрудников, всячески стараясь подготовить их к атакам на них, с каждым годом бизнес терпит огромные убытки по вине своих же сотрудников. Количество атак с использованием социальной инженерии [4] растет из года в год. Сегодня, бизнесу крайне необходимы решения, предотвращающие такие атаки и дальнейшие потери. И на данный момент DLP-системы - это самый эффективный способ решения данной проблемы. В этом и есть их уникальность. Ни одна другая система не способна так же эффективно предотвращать потери и утечки. Поэтому развитие DLP-систем в будущем способно вывести экономическую безопасность бизнеса на совершенно иной уровень.

Источники и литература

- 1) Утечки данных. Россия. 2019 год. Исследование Infowatch [Электронный ресурс]. Точка доступа: <https://www.infowatch.ru/analytics/reports/27614>
- 2) Анализ рынка информационной безопасности в России. Часть 2. [Электронный ресурс]. Точка доступа: https://www.anti-malware.ru/analytics/Market_Analysis/analysis-information-security-market-russia-part-2
- 3) Исследование «Топ 5 разочарований пользователей DLP-систем». [Электронный ресурс]. Точка доступа: <https://www.securitylab.ru/analytics/503316.php>
- 4) Митник К.Д., Саймон У. Искусство обмана. Издательство: Компания АйТи, 2004. – 416 с.