УДК 004.056.5

ИССЛЕДОВАНИЕ ДОСТОИНСТВ И НЕДОСТАТКОВ ВНЕДРЕНИЯ СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ DLP В КОММЕРЧЕСКУЮ ОРГАНИЗАЦИЮ

Сивков Д.И., СПбГУТ им. проф. М. А. Бонч-Бруевича
Научный руководитель – К.т.н, доцент кафедры ЗСС Андрианов В.И.
СПбГУТ им. проф. М. А. Бонч-Бруевича

В статье представлено исследование о основных достоинствах и недостатках внедрения системы мониторинга и предотвращения утечек информации DLP в коммерческую организацию. Целью работы является создание методики, которая необходима специалистам информационной безопасности при проектирование информационной системы с использованием DLP. Подробно представлены все достоинства и недостатки с их подробным описанием, а же проведена проектная экспертиза попытки внедрения DLP-системы в коммерческую организацию.

В 21 веке окружающая среда с каждым днем все стремительней развивается и меняется благодаря новым информационным технологиях и интернету. Продукты, позволяющие обнаруживать вторжения в информационные системы – это инструменты, помогающие управлять угрозами и уязвимостями в этой изменяющейся среде. Угрозы – это в первую очередь люди или группы лиц, которые могут поставить под угрозу вашу компьютерную систему не зависимо от масштаба. Это может быть, к примеру, любопытный подросток, недовольный сотрудник или шпионаж от конкурирующей компании или иностранного правительства. Поэтому внедрение системы защиты от утечки информации является для организации просто необходимостью в современном мире.

Поступающий объем информации на обработку во всем мире возрастает в динамическом масштабе. С целью быстрого реагирования на какие-либо изменения рынка, получения конкурентоспособных преимуществ, выработки повышенного производства требуется эффективно и быстро получать, обрабатывать и конечно же анализировать большой объем данных, а для этого нужно обеспечивать безотказность и высокую работоспособность систем. DLP-системы позволяют в реальном времени анализировать весь входящий и исходящий сетевой трафик, а так же реагировать на опасные сигнатуры.

Всегда было очевидно, что необходимо защищаться от внутренних угроз, но чаще всего приоритет отдавался защите от внешних нарушителей. В настоящее время следует констатировать, что внутренние источники угроз, такие как, сотрудники предприятий или другие лица, имеющее легальный доступ к данным столь же значимы, как и внешние.

В статье была рассмотрена статистика глобального исследование утечек конфиденциальной информации, на предмет зарегистрированных утечек информации с 2006-2019 год, а также распределение утечек по вектору воздействия, распределение утечек по виновнику, и каналам утечки за 2019 год.

Поэтому результатом данной статьи является – создание уникальной методики для специалистов занимающихся информационной безопасностью с проектной экспертизой попытки внедрения DLP-системы для предотвращения утечек информации основываясь на её достоинствах и недостатках.