Секция «Компьютерное право и информационная безопасность»

Обнаружение каналов и фактов утечки информации при помощи автоматизированных систем

Научный руководитель – Фролов Андрей Евгеньевич

Лесъкова Александра Дмитриевна

Студент (магистр)

Алтайский государственный университет, Физико-технический факультет, Кафедра прикладной физики, электроники и информационной безопасности, Барнаул, Россия

E-mail: leskova.asya@list.ru

Утечки конфиденциальной информации присущи подавляющему большинству предприятий. По статистике доля умышленных утечек в России в 2021 году составила 79,7 %, превзойдя общемировой показатель в 76,8 % [1].

В связи с этим контроль конфиденциальной информации является актуальной задачей, ведь утечка информации может повлечь за собой не только многомиллионные финансовые потери, но и нанести трудно оцениваемый репутационный ущерб. Наличие дорогостоящих систем защиты информации зачастую оказывается недостаточным для предотвращения утечек информации.

Целью данной работы является реализация эффективных механизмов предотвращение утечки конфиденциальной информации.

Защита информации от утечки - защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации [2].

Существуют три типа систем предотвращения утечки информации [3-6]:

- DLP;
- UAM;
- PAM.

На данный момент существует множество систем контроля и предотвращения утечек информации, применяемых для контроля утечек информации, имеющие сертификат ФСТЭК.

В виду специфичности отдельных функций и финансовых ограничений ддальнейшее рассмотрение производилось между программными продуктами Стахановец, Стаффкоп и InfoWatch.

В ходе сравнительного анализа был выбран программный продукт «Стахановец» как наиболее подходящий для выполнения поставленных задач. Другие программные продукты не подошли по ряду параметров среди которых присутствует ценовой показатель и отсутствие необходимого функционала.

Анализ структуры исследуемой организации показал высокие требования к вычислительным ресурсам системы. Для минимизации требований был проведен анализ текущей структуры организации и выявлены группы риска, в которую вошли ИТ служба, отдел менеджмента, отдел закупок и бухгалтерия. Помимо этого интервьюирование показало многообразие используемых технологий, являющихся потенциальными каналами утечки информации.

Анализ правил фильтрации показал отсутствие правил фильтрации трафика до каких-либо облачных ресурсов [7].

Часть обнаруженных сервисов была заблокирована в виду отсутствия активности пользователей по отношению к этим сервисам. Относительно же открытых сервисов, где был средний и высокий уровень активности, был составлен список пользователей для подключения к мониторингу UAM системы.

Заключительным этапом явилось структурирование данных и организация поиска каналов утечки информации и обнаружения фактов утечки конфиденциальных данных [8].

Углубленный анализ взаимосвязей источников [9] возникновения каналов утечки информации и фактов утечки конфиденциальной информации, явились 3 пользователя, нарушающих правила работы с конфиденциальной информацией. Один из пользователей делал это систематически.

Исходя из вышеописанных фактов, полученные результаты свидетельствуют о эффективной работе внедренной UAM системы как средства защиты от утечек информации.

Источники и литература

1) Аналитический отчет по утечкам информации (InfoWatch). 2021 [Электронный ресурс]. – Точка доступа: https://www.infowatch.ru/analytics.
2) Блинов А.М. Информационная безопасность: учебное пособие. Часть 1. –СПб.: Изд-во СПбГУЭФ, 2010. –96 с.
3) Data Loss Statistics. [Электронный ресурс]. – Точка доступа: http://www.data-lossdb.org/statistics.
4) UAM — мониторинг действия пользователей. [Электронный ресурс]. – Точка доступа: https://cloudnetworks.ru/inf-bezopasnost/uam/.
5) FUDO PAM. [Электронный ресурс]. – Точка доступа: https://channel4it.com/publications/FUDO-PAM-prostoy-i-effektivnyy-kontrol-privilegirovannyh-polzovateley-33809.html.
6) СТАХАНОВЕЦ. [Электронный ресурс]. – Точка доступа: https://stakhanovets.ru/.
7) Курило А.П., Зефиров С.А., Голованов В.Б., и др. Аудит информационной безопасности – М.: Издательская группа «БДЦ-пресс», 2011. – 304 с.
8) Артамонов В.А., Артамонова Е.В. Каналы утечки информации.// Аналитический обзор. [Электронный ресурс]. – Точка доступа: http://itzashita.ru/analitics/analiticheskij-obzor-kanaly-utechki-informacii.html
9) Доля А. Саботаж в корпоративной среде [Электронный ресурс]. – Точка доступа: http://citforum.ru/security/articles/sabotage/