УДК 004.056 https://www.doi.org/10.47813/dnit-II.2023.7.389--394 EDN MMSXSZ

Преимущества практической реализации альтернативной концепции развития DLP-систем

А.С. Александров

Аккредитованное образовательное частное учреждение высшего образования
«Московский финансово-юридический университет МФЮА»
АОЧУ ВО МФЮА, ул. Введенского, 1А, Москва, 117342, Россия

E-mail: 29395356@s.mfua.ru, alexibb1312@yandex.ru

Аннотация. Доклад посвящён системам противодействия утечкам информации – DLP-системам. Рассмотрены основные компоненты комплексного программного обеспечения, предлагаемого к разработке для реализации альтернативной концепции развития DLP-систем.

Ключевые слова: предотвращение утечки данных, DLP-система, программное обеспечение, альтернативная концепция.

Advantages of the practical implementation of the alternative concept for the development of DLP systems

A.S. Aleksandrov

Accredited private educational institution of higher education
"Moscow University of Finance and Law MFUA",
1A Vvedenskogo str., Moscow, 117342, Russia

E-mail: 29395356@s.mfua.ru, alexibb1312@yandex.ru

Abstract. The report focuses on data leak prevention systems – DLP-systems. The main components of the comprehensive software proposed for development for the implementation of the alternative concept for the development of DLP systems are considered.

Keywords: data leak prevention, DLP-system, software, alternative concept.

1. Введение

Анализ развития DLP-систем за последние несколько лет показал, что в основе их работы по-прежнему лежат методы контентного анализа и статистических технологий [1]. По заверению вендоров, за последние годы существенно возросла эффективность DLP-систем благодаря наличию встроенных элементов искусственного интеллекта [1]. Развитие получили подсистемы выявления сложных текстовых и графические объектов даже в случае, если нарушитель смог значительно видоизменить их, а затем замаскировал свои действия [2].

Однако по-прежнему можно отметить следующие недостатки основной концепции современных DLP-систем:

- Процессы мониторинга системы электронного документооборота (далее – СЭД) непосредственно встроены в бизнес-процессы информационной системы организации (далее – ИС), что в целом влияет на скорость обмена информацией, особенно с увеличением разнообразия форм ЭД;
- Основная концепция предусматривает полный контроль электронного документа (далее – ЭД) в момент пересечения им периметра зоны безопасности ИС, несмотря на то, анализировался ли данный документ ранее или нет. Поэтому, можно сделать вывод об избыточности мониторинга ЭД [3];
- Концепцией предусмотрен в основном анализ только выходящего потока ЭД;
- Архитектура существующих DLP-систем требует постоянного сопровождения при обновлениях форм ЭД, шаблонов классификации ЭД и др;
- Механизм детектирования цифровых отпечатков не в полной мере решает проблему обнаружения сложных составных ЭД, которые могут состоять из изменённых фрагментов других конфиденциальных ЭД;
- Несмотря на наличие таких механизмов, как аудит действий и разграничение прав доступа к срезам событий у администраторов безопасности (далее – сотрудников ИБ) существует возможность просматривать контент любого ЭД, что не исключает угрозу утечки информации.

Анализ представленных недостатков ранее позволил сформировать альтернативную концепцию развития DLP-систем при сохранении их отдельных существующих функций [3].

При этом, альтернативная концепция не затрагивает прочие функции современных DLP-систем, относящиеся к контролю лояльности и действий сотрудников (поведенческий анализ, снимки экрана, кейлоггеры, и т.д.) [1, 4].

2. Постановка задачи (Цель исследования)

В данной статье предлагается рассмотреть основные идеи альтернативной концепции развития DLP-систем, а также описание необходимых компонентов и преимущества её программной реализации. Статья призвана повысить интерес к предлагаемому решению с целью выработки стратегии развития DLP-систем на ближайшие годы.

3. Методы и материалы исследования

Традиционно все ЭД в СЭД можно классифицировать как:

- Входящие, которые могут содержать конфиденциальную информацию;
- ЭД, которые генерируются сотрудниками и автоматизированной системой управления;
- Сложные составные ЭД, содержащие, в том числе, конфиденциальную информацию.

Все три группы ЭД слабо чувствительны к фактору времени. Это обстоятельство учтено в альтернативной концепции DLP-систем, в которой анализ содержимого ЭД этих групп может проводиться не в жёстких условиях временных ограничений, а в момент поступления их в систему или при создании их в ИС [3]. Для этого введена дополнительная конструкция и механизм формирования описания документа (сертификата), позволяющие выполнять следующие функций:

- Сохранять историю создания и изменения ЭД, ссылки на источники составных документов, цифровые отпечатки этих включений и их координаты в документе;
- Определять авторство ЭД, в том числе для составных документов;
- Определять уровень конфиденциальности для ЭД исходя из уровня конфиденциальности его составных частей в соответствии с установленными правилами информационной безопасности [5];
- Определять допустимость устройств вывода этого ЭД в соответствии с его категорией конфиденциальности.

Кроме того, механизм сертификата в перспективе может обеспечить возможность определения наличия стегоконтейнеров.

Модель электронного документа в представленной концепции имеет следующий вид (уравнение 1):

$$\begin{cases} S = \{t_1, t_2, t_3, \ldots, t_i\}; \\ C = \{a_i, k_i, u_i, m_i, h_i, d_i, x_i, \ldots\}, \end{cases} \quad (1)$$

где: S – редактируемый/создаваемый ЭД; t_i – блоки составного ЭД; C – сертификат ЭД, a_i – автор(ы); k_i – уровень конфиденциальности; u_i – источник (адрес); m_i – матрица разрешенных действий; h_i – цифровой отпечаток; d_i – дата, время; x_i – ключевые слова, аннотация, метки и другая информация.

С учётом изложенного, данная концепция требует разработки принципиально новых программных решений (с сохранением отдельных элементов существующих DLP-систем), которые будут составлять «ядро» системы [3]:

- Программа-агент (далее – ПА) для каждого эндпоинта (рабочего места) ИС. В задачи ПА входит создание/изменение сертификата ЭД параллельно с его созданием/изменением во всех используемых офисных приложениях. Помимо этого, ПА обладает механизмом, который обеспечивает контроль её собственной целостности.
- Модуль контроля сертификатов при пересечении ЭД границы периметра безопасности. Помимо описанного целевого назначения, данное решение выполняет свою функцию, в том числе, и при появлении ЭД на границе периметра безопасности без соответствующего сертификата. В этом случае она обеспечивает немедленное блокирование передачи ЭД, приступая к запуску механизма расследования инцидента.
- Модуль автоматизированного расследования инцидентов по анализу сертификата документа. Программа, на основании исследования сертификата ЭД, обеспечивает построение графа изменения состояния документа и его исполнителей с учётом ссылок на включённые в него другие документы и источники.
- Модуль описания информационного пространства должностных лиц организации и их полномочий по доступу к документам различного уровня конфиденциальности, который обеспечивает контроль матрицы доступа к конфиденциальной информации разного уровня в системе и меру ответственности сотрудников ИБ.

4. Полученные результаты

Дальнейшее развитие DLP-систем с учётом альтернативой концепции позволяет не только уйти от описанных ранее недостатков, но и обладает рядом конкурентных преимуществ. Проведём сравнение некоторых основных свойств DLP-систем, построенных в рамках основной и альтернативной концепции (таблица 1).

Таблица 1. Сравнение свойств DLP-систем, построенных в рамках основной и альтернативной концепции**.**

Свойство	Основная концепция[1]	Альтернативная концепция
Критичность системы ко времени контроля ЭД	Критична. За счёт контроля ЭД в момент пересечения границы периметра зоны безопасности ИС	Некритична. За счёт контроля готового сертификата ЭД при пересечении границы периметра зоны безопасности ИС.
Влияние на производительность ИС	Присутствует. За счёт избыточности мониторинга ЭД	Снижено. За счёт проверки только сертификата, где содержится вся информация о ЭД
Проактивная защита	Собор данных о движении информации и действиях сотрудников на эндпоинтах, сканирование файловых ресурсов и рабочих станции для анализа и классификации хранимой информации построение профилей пользователей и поведенческий анализ.	Сертификат ЭД уже содержит историю создания и изменения ЭД.
Особенности настройки и сопровождение системы	Сопровождение при изменениях форм ЭД, каналов, протоколов, шаблонов ЭД для их классификации и др.	Автоматическая настройка путём ввода формализованной политики безопасности с матрицей доступов и ответственности сотрудников организации при работе в ИС
Возможность ознакомления персонала службы безопасности с содержанием документа	Внедрены ограничения в виде аудита действий сотрудников ИБ, разграничение прав доступа к срезам событий.	Сотрудник ИБ видит граф изменения состояния документа, его исполнителей, ссылки на включённые в него фрагменты документов и другие источники.
Идентификация сложных составных документов	Поиск фрагментов текста, принадлежащих к заранее заданным эталонным документам.	Присутствует. За счёт анализа сертификата ЭД.
Ожидаемая совокупная стоимость владения	Спецификация оборудования для каждого случая рассчитывается отдельно на основании типа установки, предполагаемой нагрузки и параметров сети.	Ожидается ниже, чем в рамках основной концепции. За счёт снижения требований к характеристикам оборудования.
Возможность автоматизированного расследования инцидентов	Частичная. Сбор и визуализация данных для расследования инцидентов специалистами ИБ	Присутствует. На этапе формирования сертификата ЭД

[1] На примере современного DLP-решения одного из ведущих отечественных вендоров.

5. Выводы

Практическая реализация предлагаемой альтернативной концепции, которая строится не на анализе содержимого документа при пересечении периметра безопасности контролируемой зоны, а на проверке его сертификата, в котором есть вся информация о документе для принятия решения, позволяет уйти от недостатков существующих DLP-решений, уменьшить их стоимость, повысить скорость обнаружения с минимальным количеством ложных срабатываний.

Список литературы

1. Быстрова, Е. Обзор InfoWatch Traffic Monitor 7.3, системы защиты от утечек конфиденциальной информации / Е. Быстрова., [Электронная версия] – URL: https://www.anti-malware.ru/reviews/InfoWatch-Traffic-Monitor-73
2. Бугорский, М.А. Разработка модели повышения эффективности функционирования подсистемы контроля утечек изображений автоматизированной системы в защищенном исполнении за счет рационального перераспределения ресурсов / М.А. Бугорский, А.Б. Сизоненко // Вестник Воронежского института высоких технологий. – 2022. – № 4(43). – С. 20-23.
3. Минзов, А.С. Новые подходы к предупреждению утечек информации в корпоративных информационных системах / А.С. Минзов, А.С. Александров, В.А. Мещерский // Информатизация инженерного образования: Труды Международной научно-практической конференции - ИНФОРИНО-2016, Москва, 12–13 апреля 2016 года. – Москва: Издательский дом МЭИ, 2016. – С. 172-177.
4. Петренко, С.А. Развитие DLP в России: история, тенденции и перспективы // Аналитический банковский журнал. – 2014. – Т. 221. – № 09. [Электронная версия] – URL: https://iteranet.ru/press/publications/razvitie-dlp-v-rossii-istoriya-tendentsii-i-perspektivy/?ysclid=lecygphgmr145884598.
5. ГОСТ Р ИСО/МЭК 27002-2021 Информационные технологии (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности.