УДК 004.056.5 **DOI** 10.34757/2413-7383.2023.30.3.005

Е. Ю. Потреба, Н. Е. Губенко
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Донецкий национальный технический университет»
283001, г. Донецк, ул. Артёма, 58

АНАЛИЗ МЕТОДОВ И СРЕДСТВ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ

Y. Y. Potreba, N. E. Gubenko
Federal State Budgetary Educational Institution of Higher Education
"Donetsk National Technical University"
283001, Donetsk, st. Artyoma, 58

ANALYSIS OF METHODS AND MEANS OF PREVENTING CONFIDENTIAL DATA LEAKS

Ю. Ю. Потреба, Н. Є. Губенко
Донецький національний технічний університет
283050, Донецьк, вул. Артема, 58

АНАЛІЗ МЕТОДІВ І ЗАСОБІВ ЗАПОБІГАННЯ ВИТОКІВ КОНФІДЕНЦІЙНИХ ДАНИХ

В статье проведен анализ существующих методов и средств защиты конфиденциальной информации. Произведен поиск наиболее эффективных подходов, обеспечивающих безопасность конфиденциальных данных. Описаны преимущества и недостатки отобранных подходов. Классифицированы функции системы предотвращения утечек данных.
Ключевые слова: информационная безопасность, конфиденциальность, утечка данных.

The article analyzes methods and means of protecting confidential information. The search for the most effective approaches to ensure the security of confidential data has been carried out. The advantages and disadvantages of the selected approaches are described. The functions of the data leak prevention system are classified.
Key words: information security, confidentiality, data leakage.

У статті проведено аналіз існуючих методів та засобів захисту конфіденційної інформації. Проведено пошук найбільш ефективних підходів, що забезпечують безпеку конфіденційних даних. Описано переваги та недоліки відібраних підходів. Класифіковані функції системи запобігання витоків даних.
Ключові слова: інформаційна безпека, конфіденційність, витік даних.

Постановка проблемы

Сложившаяся экономическая ситуация значительно усилила конкурентную борьбу компаний за позиции на рынке, а иногда и за выживание. Буквально за несколько лет произошли значительные изменения в обществе, продолжают меняться деловая деятельность и форматы общения между людьми. Многие процессы в различных сферах жизнедеятельности принимают новые формы.

Современный мир – информационный, именно поэтому происходит активная диджитализация большинства видов предоставления услуг, продолжают внедряться электронные базы данных, цифровые формы документооборота. Расширилась деловая активность общества в целом: стали развиваться новые виды и формы коммуникации. В связи с этим актуализируется вопрос, который напрямую затрагивает информационную безопасность личности и общества, предприятий и государств.

Рассматривая информацию в разрезе предприятий и организаций, следует отметить, что это одна из основных составляющих любого бизнеса, как и любого процесса в целом – содержащая данные о производственных процессах, оборудовании, финансовой и управленческой структуре, взаимоотношении с поставщиками потребителями, дилерами и заказчиками.

Перечисленные виды информации лежат в плоскости защиты данных и информационной безопасности, однако руководство организаций и предприятий не всегда имеет полное представление о степени и видах угроз для производственно-финансовых процессов со стороны злоумышленников в комплексной информационной системе, а также об их последствиях для бизнеса. Некоторые компании, разрабатывая антикризисные стратегии, значительно сократили расходную часть по некоторым статьям своего бизнеса. Нередко, под сокращение расходов попадает информационная безопасность. Однако экономия чревата утечками персональных данных и конфиденциальной информации, что может навредить бизнесу в целом.

Так, аналитики утверждают, что более половины рисков, с которыми может столкнуться компания, составляют внутренние угрозы. В период кризиса, показатели внутренних угроз могут подниматься до 60%. Всё дело в том, что во времена экономической нестабильности происходят случаи ротации и даже увольнения кадров. По этой причине недовольные сотрудники пытаются либо перепродать важную информацию конкурентам, либо уничтожить базы данных, считая их своей собственной наработкой [0].

Ротация сотрудников всё чаще наблюдается на предприятиях, которые занимаются компьютерной разработкой: IT-компании, рекламные агентства, студии дизайна и т.д. Это связано с тем, что специалисты могут работать на проектной основе или ведут собственные проекты, поэтому работа может быть временной. Кроме того, конкуренция на рынке данных услуг высока, работники ищут новые возможности для профессионального роста.

Увольнения в дизайн-студиях могут происходить по разным причинам, включая изменение приоритетов компании, недостаточную эффективность работы сотрудника или экономические показатели. Компании также могут переживать трудности в бизнесе и вынуждены сокращать персонал. В целом, увольнения и ротация сотрудников в дизайн-студиях являются обычным явлением, и компании обычно стараются сделать процесс максимально справедливым и безопасным.

Для улучшения экономической безопасности необходимо анализировать все процессы, происходящие при взаимодействии с информацией в системах электронного документооборота. Кроме того, необходимо определить и внедрить стратегически важные инструменты для оптимизации контроля над процессами и предотвращения утечек данных.

Источники угроз конфиденциальной информации

Источниками угрозы сохранности конфиденциальных данных могут являться как компании-конкуренты и злоумышленники, так и сотрудники вместе с органами управления компанией. Цель любой угрозы заключается в том, чтобы повлиять на целостность, полноту и доступность данных.

Угрозы бывают внешними и внутренними. Внешние угрозы представляют собой попытки получить доступ к данным извне и сопровождаются взломом серверов, сетей, аккаунтов работников и считыванием информации из технических каналов утечки (акустическое считывание с помощью жучков, камер, наводки на аппаратные средства, получение виброакустической информации из окон и архитектурных конструкций).

В свою очередь, внутренние угрозы подразумевают неправомерные действия персонала, рабочего отдела или управления фирмы. В результате пользователь системы, который работает с конфиденциальной информацией, может выдать информацию посторонним. На практике такая угроза встречается чаще остальных. Работник может годами предоставлять конкурентам секретные данные. Это легко реализуется, ведь действия авторизованного пользователя администратор безопасности не квалифицирует как угрозу.

Поскольку внутренние ИБ-угрозы связаны с человеческим фактором, отслеживать их и управлять ими сложнее. Предупреждать инциденты можно с помощью деления сотрудников на группы риска.

Попытка несанкционированного доступа может происходить несколькими путями:

– через сотрудников, которые могут передавать конфиденциальные данные посторонним, забирать физические носители или получать доступ к охраняемой информации через печатные документы;
– с помощью программного обеспечения злоумышленники осуществляют атаки, которые направлены на кражу пар «логин-пароль», перехват криптографических ключей для расшифровки данных, несанкционированного копирования информации;
– с помощью аппаратных компонентов автоматизированной системы, например, внедрение прослушивающих устройств или применение аппаратных технологий считывания информации на расстоянии (вне контролируемой зоны) [3].

Для предотвращения кражи, изменения и распространения конфиденциальной информации настоятельно рекомендуется использование соответствующих комплексных программных решений.

Технологии предотвращения утечки данных

Технологии защиты от утечек информации базируются на выявлении, предотвращении, регистрации и устранении последствий инцидентов информационной безопасности или событий, нарушающих регламентированные процедуры защиты ИБ.

В рамках обеспечения информационной безопасности дизайн-студии особое внимание должно обращаться на защиту конфиденциальных данных от внутренних угроз. Таким, образом вокруг системы управления компанией должен быть создан защищенный цифровой «периметр», который будет анализировать всю исходящую, а в ряде случаев и входящую информацию.

Контролируемой информацией должен быть не только интернет-трафик, но и ряд других информационных потоков: документы, которые выносятся за пределы защищаемого контура безопасности на внешних носителях, распечатываемые на принтере, отправляемые на мобильные носители через Bluetooth и т.д. [3].

На данный момент существует множество подходов, обеспечивающих безопасность конфиденциальной информации на предприятиях. Выделим наиболее эффективные из них, и опишем их преимущества и недостатки.

а) *Endpoint Detection and Response* (EDR)

Система защиты, которая обнаруживает и предотвращает угрозы в режиме реального времени на устройствах конечных пользователей, таких как рабочие станции, ноутбуки и мобильные устройства.

Преимущества EDR:

– обнаружение угроз в режиме реального времени на конечных устройствах;
– быстрое реагирование на инциденты безопасности
– возможность удаленно блокировать устройства и удалить конфиденциальные данные.

Недостатки EDR:

– может быть сложно настроить и использовать;
– может приводить к ложным срабатывания;
– не всегда способна обнаружить новые угрозы, которые еще не были зафиксированы в базе данных [4].

б) *Cloud Access Security Broker* (CASB)

Платформа, которая обеспечивает контроль и безопасность доступа к облачным сервисам, и предотвращает утечки данных в облаке.

Преимущества CASB:

– обнаружение угроз в режиме реального времени на конечных устройствах;
– быстрое реагирование на инциденты безопасности;
– возможность удаленно блокировать устройства и удалить данные.

Недостатки CASB:

– может быть сложно настроить и использовать;
– может приводить к ложным срабатывания;
– не всегда способна обнаружить новые угрозы, которые еще не были зафиксированы в базе данных [5].

в) *User and Entity Behavior Analytics* (UEBA)

Подход к анализу поведения пользователей и сущностей, который использует машинное обучение для выявления вредоносных действий внутри сети.

Преимущества UEBA:

– обнаружение аномального поведения пользователей и сущностей;
– обнаружение скрытых угроз, которые могут быть незаметными для других систем безопасности;
– мониторинг активности пользователей и анализ угроз безопасности.

Недостатки UEBA:

– может приводить к ложным срабатываниям, если система не настроена должным образом;
– может требовать большого объема данных для обучения алгоритмов [6].

г) *Security Information and Event Management* (SIEM)

Система, которая собирает и анализирует данные о событиях безопасности в режиме реального времени, чтобы обнаружить аномалии и потенциальные угрозы безопасности.

Преимущества SIEM:

– сбор и анализ логов для обнаружения угроз безопасности;
– быстрое реагирование на инциденты безопасности;
– возможность интеграции с другими системами безопасности.

Недостатки SIEM:

– может приводить к ложным срабатываниям, если система не настроена должным образом;
– может не обнаружить новые и неизвестные угрозы, которые еще не были зафиксированы в базе данных [7].

д) Data Leak Prevention (DLP)

Набор технологий, политик и процессов, для контроля и управления информацией, предотвращая несанкционированный доступ, использование и распространение конфиденциальных данных.

Преимущества DLP:

– позволяет отслеживать и анализировать действия пользователей на рабочих местах, на серверах и в сети;
– работает в режиме реального времени и способна быстро реагировать на возникающие угрозы безопасности;
– соблюдение законодательства и стандартов, связанных с защитой данных, таких как ГОСТ Р ИСО/МЭК 27001 и 27002, HIPAA, GDPR, и т.д.

Недостатки DLP:

– ограниченность в распознавании новых угроз;
– реализация системы может быть дорогостоящей, особенно для крупных организаций с большим объемом данных [8].

Каждая из этих перечисленных систем может быть полезной в зависимости от потребностей и требований предприятий. Оценив преимущества и недостатки, а также основываясь на целях и задачах защиты конфиденциальных данных, в систему управления дизайн-студией решено внедрять методы Data Leak Prevention.

Система Data Leak Prevention

Поскольку система *Data Leak Prevention* должна препятствовать утечкам конфиденциальной информации, то она в обязательном порядке имеет встроенные механизмы определения степени конфиденциальности документа, обнаруженного в перехваченном трафике. Как правило, наиболее распространены два способа: путём анализа специальных маркеров и содержимого документа.

В настоящее время более распространен второй вариант, поскольку он устойчив перед модификациями, вносимыми в документ перед его отправкой, а также позволяет легко расширять число конфиденциальных документов, с которыми может работать система.

Принцип работы DLP-систем заключается в анализе всего трафика, который находится в пределах защищаемой корпоративной сети. Внедрение DLP-системы помогает контролировать входящие и исходящие потоки данных и блокировать попытки несанкционированной передачи важных корпоративных данных.

DLP работает по принципу *data-centric security*. Он подразумевает не защиту серверов, программного обеспечения или сетей, а контроль безопасности данных, которые обрабатываются в системе. Согласно этому принципу, все потоки информации разделяют на три категории:

– Data-in-use – вся информация, с которой работают пользователи (создание и редактирование документов, медиаконтента).
– Data-at-rest – информация, которая статично хранится на конечных устройствах пользователей и в местах общего доступа.

– Data-in-motion – данные в процессе движения, передаваемые информационные потоки (транзакции, информация об авторизации, запросы «сервер-клиент» и другие) [9].

Помимо своей основной задачи, связанной с предотвращением утечек информации, DLP-системы также хорошо подходят для решения ряда других задач, связанных с контролем действий персонала.

Наиболее часто DLP-системы применяются для решения следующих неосновных для себя задач:

– контроль использования рабочего времени и рабочих ресурсов сотрудниками;
– мониторинг общения сотрудников с целью выявления «подковерной» борьбы, которая может навредить организации;
– контроль правомерности действий сотрудников (печать поддельных документов и пр.);
– выявление сотрудников, рассылающих резюме, для оперативного поиска специалистов на освободившуюся должность [10].

При внедрении DLP-системы важно придерживаться не только принципов защиты информации, но и норм законодательства. Контроль за соблюдением правил работы с конфиденциальной информацией не должен нарушать личные права пользователей, поэтому стоит отказаться от действия, которые могут быть расценены как слежка. Дополнительно стоит предусмотреть механизмы контроля администраторов системы, у которых есть доступ ко всем типам данных. Чтобы избежать недовольства и возмущения в коллективе, в общие сведения о работе системы рекомендуется включить пункты, где четко обозначить цели внедрения DLP-контроля.

Для обеспечения максимально возможной защиты информации в процессе внедрения DLP следует выполнять все рекомендации и использовать сразу несколько блоков защиты. Это позволит создать экономически выгодный, рабочий защитный контур. Внедрение DLP-системы должно выполняться поэтапно от подготовки до проектирования и настройки компонентов для работы под нагрузкой в компании.

Классификация функций DLP-систем

Одним из весомых преимуществ при выборе стала возможность внедрения только части системы *Data Leak Prevention*, в зависимости от потребностей организации и ее бюджета.

В зависимости от потребностей организации, можно выбирать конкретные компоненты DLP-системы, которые будут наиболее полезны для решения конкретных задач. Например, если в организации есть потребность в защите конфиденциальной информации при передаче ее через электронную почту, можно установить специализированный компонент DLP для мониторинга и анализа электронных сообщений.

DLP системы могут включать в себя следующие функции:

– мониторинг сетевого трафика и систем, обнаружение необычных активностей и отслеживание передачи конфиденциальных данных;
– фильтрация контента и блокирование нежелательных сайтов и приложений, а также контроль использования внешних носителей;
– контроль доступа и авторизации сотрудников на основе ролей и прав доступа;
– шифрование данных и аудит действий пользователей;
– анализ и классификация данных, определение уровня конфиденциальности.
– управление политиками безопасности и обеспечение соответствия стандартам и законодательству.

Реализация отдельных методов DLP-системы может повысить уровень безопасности и защиты конфиденциальной информации, уменьшить риски утечки и повысить доверие клиентов и партнеров. Однако, важно учитывать, что DLP-система будет более эффективной и защищенной, если будет использоваться в полном объеме и с настройками, оптимизированными под конкретные потребности организации [11].

Выводы

Проведен анализ существующих методов и средств защиты конфиденциальной информации. Произведен поиск наиболее эффективных подходов, обеспечивающих безопасность конфиденциальных данных. Описаны преимущества и недостатки отобранных подходов.

Отмечено, что каждая из перечисленных систем может быть полезной в зависимости от потребностей и требований предприятий. Основываясь на целях и задачах защиты конфиденциальных данных, в систему управления предприятием решено внедрять методы Data Leak Prevention.

К основным функциям системы DLP относятся: мониторинг сетевого трафика и систем, обнаружение необычных активностей и отслеживание передачи конфиденциальных данных, фильтрация контента и блокирование нежелательных сайтов и приложений, а также контроль использования внешних носителей, контроль доступа и авторизации сотрудников на основе ролей и прав доступа, шифрование данных и аудит действий пользователей.

Внедрение методов DLP позволит обеспечить максимальную защиту конфиденциальных данных и создать экономически-выгодный защитный контур предприятия.

Список литературы

1. DLP-системы — элемент ИБ [Электронный ресурс]. Режим доступа: https://www.azone-it.ru/dlp-sistemy-vazhnaya-sostavlyayushchaya-informacionnoy-bezopasnosti-predpriyatiya
2. Основы информационной безопасности [Электронный ресурс]. Режим доступа: https://цбис.рф/osnovy-informatsionnoj-bezopasnosti
3. Предотвращение утечек данных [Электронный ресурс]. Режим доступа: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems
4. EDR — обнаружение и реагирование на угрозы конечной точки [Электронный ресурс]. Режим доступа: https://cloudnetworks.ru/inf-bezopasnost/edr/
5. Брокеры безопасного облачного доступа (CASB) [Электронный ресурс]. Режим доступа: https://www.anti-malware.ru/security/casb
6. Системы поведенческого анализа – User and Entity Behavioral Analytics (UEBA) [Электронный ресурс]. Режим доступа: https://cisoclub.ru/sistemy-povedencheskogo-analiza-user-and-entity-behavioral-analytics-ueba/
7. Security Information and Event Management (SIEM) [Электронный ресурс]. Режим доступа: https://www.tadviser.ru/index.php
8. Предотвращение утечек информации с помощью DLP-систем [Электронный ресурс]. Режим доступа: https://vc.ru/u/1193668-fenixhost/453548-predotvrashchenie-utechek-informacii-s-pomoshchyu-dlp-sistem
9. Информационная безопасность. Защита данных с помощью DLP-системы [Электронный ресурс]. Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy
10. Внедрение DLP-системы на предприятии [Электронный ресурс]. Режим доступа: https://spravochnick.ru/informatika/vnedrenie_dlp-sistemy_na_predpriyatii
11. DLP – защита от утечек информации [Электронный ресурс]. Режим доступа: https://cloudnetworks.ru/inf-bezopasnost/dlp/
12. Влияние цифровых технологий на экономические и социальные аспекты / Е. М. Кот, И. Ф. Пильникова, А. А. Крохалев, Л. Н. Пильников, Р. М. Исматулаева. *Образование и право*. 2023. № 6. С. 238-241.

13. Румянцев, В. В. О роли информационных технологий в развитии цивилизации. *Проблемы искусственного интеллекта*. 2021. № 4 (23). С. 59-64.
14. Страхов А. А., Дубинина Н. М. Об утечке данных и DLP-системах // Криминологический журнал. – 2022. – № 4. – С. 226-232.
15. Дмитрюк, Т. Г., Зори, С. А. Анализ структуры производственной деятельности предприятия как объекта управления. *Проблемы искусственного интеллекта*. 2020. № 1 (16). С. 37-53.
16. Аусилова, Н. М., Зарынбеков, А. Б., Ахмет, Г. Б. Применение DLP-систем как инструмента обеспечения информационной безопасности. *Наука и реальность*. 2023. № 1 (13). С. 93-96.
17. Дорохина, Г. В. Требования к информационной технологии цифрового сбора, обработки и анализа данных. *Проблемы искусственного интеллекта*. 2020. № 4 (19). С. 4-9.
18. Ларионова, С. Л., Товпеко Л. И. Метод принятия решений в условиях неопределенности для обеспечения информационной безопасности. *Инновации и инвестиции*. 2020. С. 114-118.
19. Анцыферов С. С., Сигов, А. С. Технологические основы построения интеллектуальных систем. *Проблемы искусственного интеллекта*. 2016. № 1 (2). С. 34-44.
20. Митюшин, Д. А. Правовые вопросы применения систем защиты от утечки конфиденциальной информации на объектах информатизации. *Вестник Московского университета МВД России*. 2020. № 5. С. 163-168.
21. Румянцев, В. В. Иерархия интеллектуальных систем. *Проблемы искусственного интеллекта*. – 2018. – № 1 (8). – С. 23-31.
22. Чуб, В. С., Галушка, В. В. Исследование реализации применения стенографических методов в DLP-системе. *Молодой исследователь Дона* – 2019.
23. Дурандина, А. П. Экономико-организационные аспекты использования систем противодействия утечкам данных. *Петербургский экономический журнал*. 2021. № 1. С. 132-138.

References

1. DLP systems are an element of information security [Electronic resource]. Access mode: https://www.azone-it.ru/dlp-sistemy-vazhnaya-sostavlyayushchaya-informacionnoy-bezopasnosti-predpriyatiya
2. Fundamentals of information security [Electronic resource]. Access mode: https://цбис.рф/osnovy-informatsionnoj-bezopasnosti
3. Prevention of data leaks [Electronic resource]. Access mode: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/dlp-systems
4. EDR — detection and response to endpoint threats [Electronic resource]. Access mode: https://cloudnetworks.ru/inf-bezopasnost/edr/
5. Brokers of secure cloud access (CASB) [Electronic resource]. Access mode: https://www.anti-malware.ru/security/casb
6. Behavioral Analysis Systems – User and Entity Behavioral Analytics (UEBA) [Electronic resource]. Access mode: https://cisoclub.ru/sistemy-povedencheskogo-analiza-user-and-entity-behavioral-analytics-ueba/
7. Security Information and Event Management (SIEM) [Electronic resource]. Access mode: https://www.tadviser.ru/index.php/ Статья:Security_Information_and_Event_Management_(SIEM)
8. Prevention of information leaks using DLP systems [Electronic resource]. Access mode: https://vc.ru/u/1193668-fenixhost/453548-predotvrashchenie-utechek-informacii-s-pomoshchyu-dlp-sistem
9. Information security. Data protection using a DLP system [Electronic resource]. Access mode: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy
10. Introduction of a DLP system at the enterprise [Electronic resource]. Access mode: https://spravochnick.ru/informatika/vnedrenie_dlp-sistemy_na_predpriyatii
11. DLP — protection against information leaks [Electronic resource]. Access mode: https://cloudnetworks.ru/inf-bezopasnost/dlp/
12. Kot E. M. The influence of digital technologies on economic and social aspects / E. M. Kot, I. F. Pilnikova, A. A. Krokhalev, L. N. Pilnikov, R. M. Ismatulayeva. *Education and Law*. 2023. No. 6. pp. 238-241.
13. Rumyantsev V. V. On the role of information technologies in the development of civilization / V. V. Rumyantsev. *Problems of artificial intelligence*. 2021. № 4 (23). Pp. 59-64.

14. Strakhov A. A. On data leakage and DLP systems / A. A. Strakhov, N. M. Dubinina. *Criminological Journal*. 2022. No. 4. pp. 226-232.
15. Dmitryuk T. G. Analysis of the structure of the production activity of an enterprise as an object of management / T. G. Dmitryuk, S. A. Zori. *Problems of artificial intelligence*. 2020. № 1 (16). Pp. 37-53.
16. Ausilova N. M. Application of DLP systems as a tool for ensuring information security / N. M. Ausilova, A. B. Zarynbekov, G. B. Akhmet. *Science and Reality*. 2023. № 1 (13). Pp. 93-96.
17. Dorokhina G. V. Requirements for information technology of digital data collection, processing and analysis / G. V. Dorokhina. *Problems of artificial intelligence*. 2020. № 4 (19). Pp. 4-9.
18. Larionova S. L. The method of decision-making under uncertainty to ensure information security / S. L. Larionova, L. I. Tovpeko. *Innovation and investment*. 2020. pp. 114-118.
19. Antsyferov S. S. Technological foundations of building intelligent systems / S. S. Antsyferov, A. S. Sigov. Problems of artificial intelligence. 2016. № 1 (2). Pp. 34-44.
20. Mityushin D. A. Legal issues of application of protection systems against leakage of confidential information at informatization facilities / D. A. Mityushin. *Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia*. 2020. No. 5. pp. 163-168.
21. Rumyantsev V. V. Hierarchy of intelligent systems / V. V. Rumyantsev. *Problems of artificial intelligence*. 2018. № 1 (8). Pp. 23-31.
22. Chub V. S. The study of the implementation of the use of shorthand methods in the DLP system / V. S. Chub, V. V. Galushka. *Young researcher Don* - 2019.
23. Durandina A. P. Economic and organizational aspects of the use of anti-data leakage systems / A. P. Durandina. *St. Petersburg Economic Journal*. 2021. No. 1. pp. 132-138.

RESUME

Y. Y. Potreba, N. E. Gubenko

Analysis of methods and means of preventing confidential data leaks

Ensuring information security at the enterprise is a resource–intensive, but of paramount importance process. To improve economic security, it is necessary to analyze all interactions with information in electronic document management systems. In addition, it is necessary to identify and implement strategically important tools to optimize process control and prevent data leaks.

At the moment, there are many approaches that ensure the security of confidential information in enterprises. Each of these systems can be useful depending on the needs and requirements. The decision on the implementation of methods in the enterprise management system should be made after evaluating the advantages and disadvantages, as well as based on the goals and objectives of protecting confidential data.

The introduction of data leakage prevention technologies makes it possible to ensure maximum protection of confidential data and create an economically advantageous protective contour of the enterprise.

The implementation of separate methods of data leakage prevention systems can increase the level of security and protection of confidential information, reduce the risks of leakage and increase the trust of customers and partners. However, it is important to take into account that the DLP system will be more efficient and secure if it is used in full and with settings optimized for the specific needs of the organization.

РЕЗЮМЕ

Е. Ю. Потреба, Н. Е. Губенко

Анализ методов и средств предотвращения утечек конфиденциальных данных

Обеспечение информационной безопасности на предприятии – ресурсоемкий, но первостепенно важный процесс. Для улучшения экономической безопасности необходимо анализировать все взаимодействия с информацией в системах электронного

документооборота. Кроме того, необходимо определить и внедрить стратегически важные инструменты для оптимизации контроля над процессами и предотвращения утечек данных.

На данный момент существует множество подходов, обеспечивающих безопасность конфиденциальной информации на предприятиях. Каждая из этих систем может быть полезной в зависимости от потребностей и требований. Решение о внедрении методов в систему управления предприятием необходимо принимать, оценив преимущества и недостатки, а также основываясь на целях и задачах защиты конфиденциальных данных.

Внедрение технологий предотвращения утечек данных позволяет обеспечить максимальную защиту конфиденциальных данных и создать экономически-выгодный защитный контур предприятия.

Вывод: Реализация отдельных методов систем предотвращения утечек данных может повысить уровень безопасности и защиты конфиденциальной информации, уменьшить риски утечки и повысить доверие клиентов и партнеров. Однако, важно учитывать, что DLP-система будет более эффективной и защищенной, если её использовать в полном объеме и с настройками, оптимизированными под конкретные потребности организации

.

Губенко Наталия Евгеньевна – доцент кафедры компьютерного моделирования и дизайна, Федеральное государственное бюджетное образовательное учреждение высшего образования «Донецкий национальный технический университет», *Область научных интересов:* компьютерные информационные технологии, компьютерная безопасность, современные образовательные технологии, эл. почта negubenko@mail.ru, адрес: 283001, г. Донецк, ул. 25-летия РККА, д. 16, кв.31 телефон +7949 402 42 93

Потреба Ефим Юрьевич – магистр кафедры компьютерного моделирования и дизайна, Федеральное государственное бюджетное образовательное учреждение высшего образования «Донецкий национальный технический университет», *Область научных интересов:* компьютерные информационные технологии и дизайн, компьютерная безопасность, эл. почта potrebart@gmail.com, адрес: 283001, г. Донецк, ул. Артема, 58 телефон +7949 361 04 60

Статья поступила в редакцию 16.03.2023.