Гуреев В.А., Храмцов О.В., Тимофеев А.М. Исследование актуальности Data Loss Prevention системы в условиях дистанционной работы// Международный журнал информационных технологий и энергоэффективности.– 2024. – Т. 9 № 6(44) с. 16–25

Международный журнал информационных технологий и энергоэффективности

Сайт журнала:
http://www.openaccessscience.ru/index.php/ijcse/

УДК 004.056

ИССЛЕДОВАНИЕ АКТУАЛЬНОСТИ DATA LOSS PREVENTION СИСТЕМЫ В УСЛОВИЯХ ДИСТАНЦИОННОЙ РАБОТЫ

[1]Гуреев В.А., Храмцов О.В., Тимофеев А.М.
ФГБОУ ВО САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ ИМ. ПРОФЕССОРА М. А. БОНЧ-БРУЕВИЧА, Санкт-Петербург, Россия (193232, г. Санкт-Петербург, просп. Большевиков, 22, корп. 1), e-mail: [1]gureevvadim62@gmail.com

В данной статье рассмотрена актуальность такого средства обеспечения информационной безопасности данных, как Data Loss Prevention системы в непростое время пандемии, в условиях применения дистанционных технологий. Также было проведено небольшое описание и сравнение Data Loss Prevention систем, представленных на Российском и международном рынке.

Ключевые слова: DLP системы, безопасность данных, информационная безопасность, дистанционная работа, предотвращение потери данных.

THE STUDY OF THE RELEVANCE OF THE DATA LOSS PREVENTION SYSTEM IN THE CONTEXT OF REMOTE WORK

[1]Gureev V.A., Khramtsov O.V., Timofeev A.M.
ST. PETERSBURG STATE UNIVERSITY OF TELECOMMUNICATIONS NAMED AFTER PROFESSOR M. A. BONCH-BRUEVICH, St. Petersburg, Russia (193232, St. Petersburg, ave. Bolshevikov, 22, bldg. 1), e-mail: [1]gureevvadim62@gmail.com

This article examines the relevance of such a means of ensuring information security of data as the Data Loss Prevention system in a difficult time of the pandemic, in the context of the use of remote technologies. A short description and comparison of Data Loss Prevention systems presented on the Russian and international markets was also carried out.

Keywords: DLP systems, data security, information security, remote operation, data loss prevention.

С развитием технических систем, человек стремится создать максимально комфортные условия работы для себя. Применения дистанционных технологий позволяет сотруднику выполнять поставленные задачи, находясь не на рабочем месте. Так же причина дистанционного режима работы может быть связана с болезнью работника или не благоприятной ситуацией в стране, например с пандемией. Тут перед работодателем встает вопрос о защите конфиденциальных данных компании. Так как сотрудник работает из дома его часы, проведенные за работой, контролируются им же, вдобавок его персональный компьютер имеет доступ к данным организации. Работодатель заинтересован в защите данных от утечек и контроле своих сотрудников. Системы Data Loss Prevention способны подключаться на расстоянии к рабочим столам персональных компьютеров, что позволит в режиме реального времени проконтролировать работу работника. Система может

фиксировать распечатывание документов и их копирование, отправку сообщений на неизвестные или личные электронные адреса. Важно понимать, что утечка данных может нанести серьезный вред организации. Data Loss Prevention так же может использоваться в условиях очной работы сотрудников для защиты данных компании и контроля сотрудников. Применение этой системы сократит риски утечки данных по неосторожности или злому умыслу. Так же можно выделить неочевидные способы использование этой системы. Обеспечение юридической поддержки. Задача DLP состоит не только в том, чтобы предотвратить утечки, но еще и при наличии судебного разбирательства, предоставить доказательства злоумышленной деятельности. DLP как инструмент мотивации. Когда сотрудники осознают, что их трудовая деятельность находится под мониторингом, появляется большая ответственность за рабочий процесс. И это в свою очередь приводит к улучшению климата в коллективе. Как хранилище. DLP-технология гарантирует сохранность всей информации, поскольку содержит в своём архиве все коммуникации сотрудников, к которым в случае необходимости можно будет обратиться. Целью данной работы является исследование актуальности Data Loss Prevention систем в условиях применения дистанционных технологий [1].

Что же такое DLP система

DLP-система — специализированное программное обеспечение, предназначенное для защиты компании от утечек информации. Эта аббревиатура на английском расшифровывается как Data Loss Prevention (предотвращение потери данных) или Data Leakage Prevention (предотвращение утечки данных). [7]

Какие DLP системы уже есть на рынке

Falcongaze SecureTower

SecureTower — это DLP система 2 в 1 (Защита от утечек данных + контроль активности пользователей). Клиент получает полный контроль корпоративной информации за счет мониторинга максимального числа коммуникационных каналов и протоколов передачи данных. Все действия сотрудников автоматически анализируются и, в случае выявления нарушения, система мгновенно отправляет уведомление руководителю или службе безопасности. [8]

InfoWatch Traffic Monitor

DLP-система, основанная на методах полноценного анализа контента информационных потоков, эффективно предотвращает утечки конфиденциальной информации. InfoWatch Traffic Monitor демонстрирует высокую надежность в работе даже при значительных нагрузках на сотнях тысяч рабочих мест, способная не только мониторить, но и блокировать подозрительные действия. Система способна обнаруживать и распознавать сложные текстовые и графические объекты, даже если нарушитель попытается изменить их и скрыть свои действия. [9]

Zecurion

В комплекс Zecurion DLP входят средства для решения различных задач в рамках защиты информации, которые тесно интегрируются друг с другом в любой комбинации и составляют единую систему защиты от утечек. Все четыре системы могут использоваться самостоятельно для решения специальных задач и в то же время дополняют друг друга. Zgate, Zlock, Zdiscovery и Zserver управляются из единой консоли Zconsole с общим удобным интерфейсом. [10]

Symantec

Защита данных по всем каналам утечек: облака, электронная почта, веб-сайты, рабочие станции и серверы, системы хранения. Комплексные технологии детектирования с минимальным числом ложных срабатываний. Единая консоль для управления политиками, реагирования на инциденты, создания отчетов и администрирования. Поддержка множества продуктов для анализа поведения пользователей, шифрования, классификации данных и управления правами доступа. [11]

Solar Dozor

Высокопроизводительная DLP-система для блокирования утечек информации, контроля коммуникаций сотрудников и выявления признаков корпоративного мошенничества. Ее возможности обеспечивают контроль коммуникаций сотрудников, блокировку или изменение нежелательных сообщений, выявление и мониторинг групп риска, а также ретроспективный анализ архива коммуникаций для проведения расследований. Кроме этого, Solar Dozor может анализировать поведение пользователей (User Behavior Analytics). [12]

МФИ Софт – Гарда Предприятие

Аппаратно-программный комплекс для контроля и анализа информационных потоков компании, защиты и предотвращения утечек конфиденциальной информации. Решение совмещает в себе классические инструменты DLP и мощные аналитические возможности. «Гарда Предприятие» разработана для реализации ежедневных задач ИБ/ЭБ/HR-специалистов — она автоматизирует рутинную работу и позволяет видеть полную картину коммуникаций в любой момент времени. [13]

Сравнение DLP систем

Для сравнения систем была составлена таблица (Таблица 1).

Таблица 1 – Сравнение DLP систем

Название	**Falcongaze SecureTower**	**InfoWatch Traffic Monitor**	**Zecurion**	**Symantec**	**Solar Dozor**	**МФИ Софт – Гарда Предприятие**
Потребители	Крупные фирмы и небольшие предприятия	Компании как маленькие, так и крупные	Государственный сектор, компании могут быть как маленькие, так и крупные	Крупнейшие корпорации, насчитывающие до 100 тысяч работников	Государственные предприятия и крупные компании	Бизнес среднего и крупного уровня
Предоставление услуг	Техподдержка, помощь по внедрению, проведение обучения, а также оказание	Услуги консалтинга в системе информационной безопасности	Проведение аудита, оказание консалтинговых услуг, оказание техподдер	Обучение персонала при помощи партнеров, внедрение	Наличие технической поддержки, возможность пройти партнерское и клиентское обучение,	Возможность проведения удаленного обучения, оказание техническо

	помощи по формированию информационной защиты в организации		жки, проведение обучения		услуги консалтинга и аутсорсинга	й поддержки
Язык панели управления	Русский, английский, французский, испанский, итальянский, корейский, турецкий	Украинский, международный английский, русский, белорусский	Английский и русский	Английский, русский, японский, китайский, французский	Русский и английский	Только русский
Запись в журнал	+	+	+	+	+	+
Сохранение файлов (теневое копирование)	+	+	+ для Zlock и Zgate	+	+	+
Уведомление администратора	+ по электронной почте	+ по электронной почте	+ по электронной почте	+ по электронной почте регистрация событий через SMTP, Syslog сообщения	+ по электронной почте	+ по электронной почте
Блокировка соединения	Да, SMTP, HTTP, SMTPs, HTTP	Да, SMTP, HTTP(S)	все контролируемые каналы (около 150 штук)	Да, любой протокол распознанный системой	Да, SMTP, HTTP	НЕТ
Автоизменение сообщений	НЕТ	НЕТ	+	+	+	НЕТ

Актуальность внедрения DLP систем в организации

Большинство предпринимателей думает, что DLP-системы используются исключительно ради обеспечения информационной безопасности, но на самом деле DLP-системы уже давно используются не только для защиты от утечек данных. Рост объема технологий сменился их развитием по вертикали. DLP начали расти вглубь, качество анализа

и перехвата контента улучшилось. Данные из DLP теперь очень ценны для принятия любых решений по управлению бизнесом. Это позволяет не только обеспечить информационную безопасность, но и сервис для других подразделений компании — от HR до экономической безопасности.

Общие сведения о DLP-системе Falcongaze SecureTower 6.3.

Российская компания Falcongaze разработала SecureTower, DLP-систему, которая является программным продуктом, позволяющим предотвратить утечку корпоративных данных, и обладает средствами для анализа деятельности персонала. SecureTower способствует реализации комплексного подхода к обеспечению защиты конфиденциальной информации и является мощным инструментом управления репутационными, операционными и правовыми рисками. Это позволяет оптимизировать бизнес-процессы в компании и обеспечить ее информационную и экономическую безопасность. Система разделена на две части: серверную и клиентскую. В северную часть входят: центральный сервер, сервер индексирования, сервер пользователей, сервер контроля агентов, сервер обработки почты, сервер сетевого трафика, сервер ICAP, сервер распознавания, сервер безопасности и отчетности, сервер журналирования событий. Интерфейсная часть включает в себя консоль администратора и пользователя. [14]

Системные и технические требования для установки Falcongaze SecureTower.

Системные и технические требования приведены в виде таблицы (Таблица 2). [15]

Таблица 2 - Технические требования

Характеристика	Серверное оборудование	Клиентская часть (работа с консолью)	Конечные точки (для агентской схемы)
Процессор	2,2+ ГГц (4 ядра и более)	2 ГГц и выше	600 МГц и выше
Сетевые адаптеры	1 Гбит (2 адаптера при централизованном перехвате)	100 Мбит/1 Гбит	
Оперативная память	6 ГБ и более	не менее 4 ГБ	256 МБ и более
Жесткий диск	100 ГБ раздел для операционной системы и файлов SecureTower (RAID1 / RAID10); раздел для хранения перехваченных данных на RAID1 / RAID10	300 МБ свободного пространства	15-25 МБ свободного пространства
Видеокарта		поддержка DirectX 7.0 и выше (разрешение экрана 1024 x 768)	
Поддерживаемые ОС	Microsoft Windows Server 2008R2/2012/2016/2019 x64 Для сервера централизованного перехвата	Microsoft Windows Vista SP2 / 7 SP1 / 8 / 8.1 / 10 / Server 2008 R 1 / Server 2012 (x86 или x64)	Microsoft Windows XP SP3/Vista/7/8/10/Server 2003/2008/2012/2016/2019 (x86/x64)

	только Microsoft Windows Server 2008R2		
Предустановленные компоненты	Microsoft .Net Framework 4.7 Microsoft Visual C++ Redistributable 2008, 2010, 2013 и 2015 (x86 и x64)	Microsoft .Net Framework 4.7 Microsoft Visual C++ Redistributable 2008, 2010, 2013 и 2015 (x86 и x64)	

Функции Falcongaze SecureTower для предотвращения утечек информации.

В DLP-системе Falcongaze SecureTower выделяются следующие функции. Выявление утечек конфиденциальной информации и инсайдерской деятельности. Контроль каналов передачи данных и действий сотрудников на их рабочих компьютерах. Блокировка портов подключения, доступа веб-ресурсов и запуска приложений. Анализ контента пересылаемых файлов, в том числе текст, изображения и аудиофайлы. Расследование инцидентов информационной безопасности, причин нарушений правил безопасности. Так же можно выделить неявные функции системы. Например, Сотрудники, осознавая факт их контроля, будут более ответственно подходить к своей работе, стараясь не совершать ошибок. Более того компания сможет проанализировать рабочий день сотрудников, что поможет оптимизировать их работу. [16]

Преимущества и недостатки Falcongaze SecureTower 6.3.

Преимущества:

- Высокая скорость внедрения при наличии всех классических технологий контроля;
- Наличие широкого спектра возможностей для блокировки;
- Поддержка контроля различных мессенджеров;
- Широкое функциональное оснащение для перехвата и обработки траффика;
- Контроль многочисленных каналов обмена данными;
- Возможность наблюдения за деятельностью работников на рабочем месте;
- Удобная, наглядная отчетная система, в которой есть функция создания собственного отчета;
- Интерактивные графические анализаторы для мониторинга контактов сотрудника;
- Быстрый поиск по перехваченным данным;
- Ведение архива коммуникации сотрудников;
- Распознавание печатей и текста на изображениях;
- Низкие системные требования;
- Простой интерфейс и гибкие настройки системы.

Недостатки:

- Блокировка принтера невозможна;
- Отсутствие блокировки каналов сетевой связи;
- Отсутствует интерфейс для мобильных устройств;
- Отсутствие спецагента для мобильных ОС;
- Отсутствует подтверждение присутствия в реестре отечественного ПО.

Применение DLP-системы в условиях дистанционных технологий.

Актуальность применения дистанционных технологий на предприятиях выражается в повышении эффективности работника. Сотруднику не нужно тратить время на дорогу до места работы, так же находясь в служебной командировке, он может продолжить выполнять свои обязанности. Более того применение дистанционных технологий не всегда добровольное решение компании. В 2020г. из-за пандемии, на удаленную работы были отправлены большое количества предприятий. Компании, которые не имели возможность обеспечить достаточные условия работы для сотрудников удаленно, столкнулись с трудностями и понесли финансовые потери. По данным аудиторской компании FinExpertiza, за весну 2020 года более трети Российских организаций оказались в убытке на 1,65 трлн рублей, а остальные заработали 3,05 трлн рублей. В итоге прибыль российского бизнеса составила 1,4 трлн рублей, это на 67 % меньше, чем весной прошлого года. [17]

DLP-система в условиях дистанционных технологий.

В условиях применения дистанционных технологий подразумевается, что сотрудник будет работать на своем домашнем компьютере, следовательно, будет иметь доступ к данным предприятия. Поднимается проблема о безопасности компании и утечки персональной информации.

Для решения вышесказанных проблем предлагается рассмотреть DLP-систему Falcongaze SecureTower 6.3, как инструмент защиты компании в условиях дистанционных технологий.

Инструменты контроля Falcongaze SecureTower в условиях дистанционных технологий.

Из пяти основных функций DLP-системы Falcongaze SecureTower можно выделить четыре: выявление, контроль, анализ, расследование. Выявление утечек важная функция которая остается актуальной в условиях дистанционных технологий, так как DLP-система способна фиксировать нарушения со стороны сотрудника, он не сможет выкрасть сведения организации незаметно. Falcongaze SecureTower способен контролировать работников, проверяя их деятельность в период рабочего времени. DLP-система может подключаться к рабочему столу сотрудника, что позволит проверить добросовестное выполнение работы в режиме реального времени и при необходимости принять меры. Функция анализа позволит оптимизировать работу предприятия, выявить недостатки рабочего дня. Расследование включает в себя сохранения трафика всех рабочих, их электронные письма и действия. Это поможет предоставить доказательства в случаи необходимости. Функция блокировки портов считается не актуальной, так как предприятие не может пойти на ограничение доступа сотрудника к собственному компьютеру.

Так же остается актуальным неявное влияние DLP-системы, сотрудник будет качественнее выполнять свою работу, зная, что за ним видеться контроль. Работодатель же найдет проблемные места и сможет улучшить условия работы подчинённых в условиях дистанционных технологий. Например, удлинить или же укоротить рабочий день.

Заключение

С развитием технологий, появилась возможность выполнять работу, не находясь на рабочем месте. В связи с этим появились проблемы и вопросы связанные с безопасностью предприятия. Предложенная в данной статье DLP-система, рассматривается как инструмент защиты в условиях дистанционных технологий. Программа способна обеспечить высокую

информационную безопасность для компании, имея множества различных функций защиты и контроля, более того система способна решать широкий спектр бизнес-задач, не связанных с ее прямой целью. В условиях удаленной работы Falcongaze SecureTower 6.3 закрывает слабые места IT-безопасности и держит под контролем не только данные, но и каждого сотрудника, фиксируя нарушения. Используя рассмотренную в данной статье DLP-систему предприятия смогут, не только справиться с трудностями удаленной работы, но и оптимизировать свой график для максимального достижения целей.

Список литературы

1. В. В. Андрианов С. Л. Зефиров В. Б. Голованов Н. А. Голдуев Обеспечение информационной безопасности бизнеса//Информационная безопасность: науч.-техн. книга: электр. версия. 2010. С. 265. URL: https://pqm-online.com/assets/files/lib/books/andrianov.pdf. Дата публикации: 2010.
2. Боридько И. С., Забелиский А. А., Коваленко Ю. И. Применение DLP-систем для защиты персональных данных. // Безопасность информационных технологий: науч.-техн. журнал: электр. версия. 2012. С. 20-24. URL: https://bit.mephi.ru/index.php/bit/article/view/424. Дата публикации: 2012. Режим доступа: для зарегистрир. пользователей
3. Российская Федерация. Законы. Конституция РФ (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). послед. ред.//КонсультантПлюс: сайт. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/. (дата обращения: 22.03.2024). Режим доступа: для зарегистрир. пользователей
4. Каскинов И.И. Галимов Р.Р. Анализ эффективности DLP-систем//В сборнике: современные информационные технологии в науке. 13.11.2014. С. 128-130. URL: https://elibrary.ru/item.asp?id=22566563. Дата публикации: 13.11.2014.
5. Каширина Е.А. DLP-системы как средство защиты информации // конференция: роль и место информационных технологий в современной науке Саранск, 03.02.2016. С. 17-19. URL: https://elibrary.ru/item.asp?id=25358627. Дата публикации: 03.02.2016.
6. Российская Федерация. Законы. Приказ ФСТЭК России от 14 марта 2014 г. N 31. : послед. ред.//ФСТЭК России: сайт. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. (дата обращения: 22.03.2024).
7. Solar Dozor: офиц. сайт. URL: https://rt-solar.ru/products/solar_dozor/blog/2080. (дата обращения: 22.03.2024).
8. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/product/what-is-the-secure-tower-dlp-system/. (дата обращения: 22.03.2024).
9. Infowatch. офиц. сайт. URL: https://www.infowatch.ru/products/traffic-monitor. (дата обращения: 22.03.2024).
10. Zecurion. офиц. сайт. URL: https://www.zecurion.ru/products/zlock/description/dlp-solution/. (дата обращения: 22.03.2024).
11. Symbuy. офиц. сайт. URL: https://www.symbuy.ru/files/Symantec-DLP.pdf. (дата обращения: 22.03.2024).
12. Solar Dozor: офиц. сайт. URL: https://rt-solar.ru/products/solar_dozor/ (дата обращения: 22.03.2024).

13. Gardatech. офиц. сайт. URL: https://gardatech.ru/produkty/gp/. (дата обращения: 22.03.2024).
14. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/support/documentation/quick-start/general-information/system-structure.html
15. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/product/tech-info/. (дата обращения: 22.03.2024).
16. Falcongaze. офиц. сайт. URL: https://falcongaze.com/ru/. (дата обращения: 22.03.2024).
17. Sberbank. офиц. сайт. URL: https://www.sberbank.ru/ru/s_m_business/pro_ business/poteri-rossijskogo-biznesa-ot-koronavirusa (дата обращения: 22.03.2024).

References

1. V. V. Andrianov S. L. Zefirov V. B. Golovanov N. A. Golduev Ensuring business information security // Information security: scientific and technical. Book: elektr. version. 2010. Pp. 265. URL: https://pqm-online.com/assets/files/lib/books/andrianov.pdf . Date of publication: 2010.
2. Boridko I. S., Zabelisky A. A., Kovalenko Yu. I. Application of DLP systems for personal data protection. // Information technology security: scientific and technical Magazine: elektr. version. 2012. Pp. 20-24. URL: https://bit.mephi.ru/index.php/bit/article/view/424 . Date of publication: 2012. Access mode: for registration. users
3. The Russian Federation. Laws. The Constitution of the Russian Federation (adopted by popular vote on 12.12.1993 with amendments approved during the all-Russian vote on 07/01/2020). last ed.//ConsultantPlus: website. URL: https://www.consultant.ru/document/cons_doc_LAW_28399/. (date of application: 03/22/2024). Access mode: for registration. users
4. Kaskinov I.I. Galimov R.R. Efficiency analysis of DLP systems // In the collection: modern information technologies in science. 13.11.2014. Pp. 128-130. URL: https://elibrary.ru/item.asp?id=22566563 . Date of publication: 13.11.2014.
5. Kashirina E.A. DLP-systems as a means of information protection // conference: the role and place of information technologies in modern science Saransk, 02/03/2016. pp. 17-19. URL: https://elibrary.ru/item.asp?id=25358627 . Date of publication: 02/03/2016.
6. Russian Federation. Laws. Order of the FSTEC of Russia dated March 14, 2014 N 31.: last ed.//FSTEC of Russia: website. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. (date of access: 03/22/2024).
7. Solar Dozor: official website. URL: https://rt-solar.ru/products/solar_dozor/blog/2080. (date of access: 03/22/2024).
8. Falcongaze. ofic. website. URL: https://falcongaze.com/ru/product/what-is-the-secure-tower-dlp-system/. (date of access: 03/22/2024).
9. Infowatch. ofic. website. URL: https://www.infowatch.ru/products/traffic-monitor. (date of access: 03/22/2024).
10. Zecurion. ofic. website. URL: https://www.zecurion.ru/products/zlock/description/dlp-solution/. (date of access: 03/22/2024).
11. Symbuy. ofic. website. URL: https://www.symbuy.ru/files/Symantec-DLP.pdf. (date of application: 03/22/2024).
12. Solar Dozor: official website. URL: https://rt-solar.ru/products/solar_dozor / (date of access: 03/22/2024).

13. Gardatech. ofic. website. URL: https://gardatech.ru/produkty/gp/. (date of access: 03/22/2024).
14. Falcongaze. ofic. website. URL: https://falcongaze.com/ru/support/documentation/quick-start/general-information/system-structure.html
15. Falcongaze. ofic. website. URL: https://falcongaze.com/ru/product/tech-info/. (date of access: 03/22/2024).
16. Falcongaze. ofic. website. URL: https://falcongaze.com/ru /. (date of access: 03/22/2024).
17. Sberbank. ofic. website. URL: https://www.sberbank.ru/ru/s_m_business/pro_ business/poteri-rossijskogo-biznesa-ot-koronavirusa (date of access: 03/22/2024).