УДК *004.056.5*

Р. Ю. Донец, Н.И. Глухов

Иркутский государственный университет путей сообщения, г. Иркутск, Российская Федерация

РОЛЬ DLP-СИСТЕМ В ЗАЩИТЕ ОТ УТЕЧЕК КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

Аннотация. *В данной статье рассмотрены основные понятия в области защиты информации, связанные с утечкой информации. Описаны наиболее распространённые причины утечки конфиденциальной информации, такие как: непреднамеренное или небрежное раскрытие данных, инсайдерские угрозы и угрозы злоумышленников, целью которых является доступ к конфиденциальным данным. Вопрос рассматривается для DLP-систем. Использование DLP-системы актуально для организаций, где утечка конфиденциальной информации может привести к серьезному финансовому или репутационному ущербу, а также для организаций, которые строго относятся к лояльности своих сотрудников. Решения данного класса позволяют в полной мере защитить конфиденциальную информацию. Основные функции DLP-систем включают в себя: мониторинг, фильтрацию потоков данных, ведение отчетов, которые позволяют эффективнее реагировать на инциденты, а также проведение анализа уязвимостей и подозрительных действий сотрудников. При внедрении подобных систем в информационную систему организации необходимо правильно настроить политику безопасности, чтобы предотвратить утечку конфиденциальной информации и не нарушить законодательство. Внедряя DLP-систему в информационную систему организации, важно проинформировать работников, что позволяет предотвратить утечки конфиденциальной информации и носит профилактический характер.*

Ключевые слова: *DLP системы, утечка конфиденциальной информации, защита от утечки данных.*

R. Y. Donets , N.I. Glukhov

Irkutsk State Transport University, Irkutsk, the Russian Federation

THE ROLE OF DLP SYSTEMS IN PROTECTING AGAINST LEAKS OF CONFIDENTIAL INFORMATION OF THE ORGANIZATION

Abstract. *This article discusses the basic concepts in the field of information security related to information leakage. The most common reasons for the leakage of confidential information are described, such as: unintentional or negligent disclosure of data, insider threats and threats of intruders whose purpose is to access confidential data. The issue is considered for DLP systems. The use of the DLP system is relevant for organizations where the leakage of confidential information can lead to serious financial or reputational damage, as well as for organizations that strictly treat the loyalty of their employees. Solutions of this class allow you to fully protect confidential information. The main functions of DLP systems include: monitoring, filtering data flows, maintaining reports that allow you to respond more effectively to incidents, as well as analyzing vulnerabilities and suspicious actions of employees. When implementing such systems into an organization's information system, it is necessary to properly configure the security policy in order to prevent the leakage of confidential information and not to violate legislation. When implementing a DLP system into an organization's information system, it is important to inform employees, which helps prevent leaks of confidential information and is of a preventive nature.*

Keywords: *DLP systems, leakage of confidential information, protection against data leakage.*

Введение

Информация является важным активом многих организаций, и ее сохранность является ключевым фактором для эффективной деятельности. Нарушение конфиденциальности информации может сильно навредить репутации компании и даже привести к ее закрытию. Большинство потерь ценной информации связано с внутренними угрозами, такими как утечка коммерческой тайны, интеллектуальной собственности или персональных данных. В настоящее время, с ускорением цифровизации и распространением дистанционной работы, одной из наиболее актуальных угроз в области информационной безопасности является утечка конфиденциальных данных в результате несанкционированных действий пользователей информации. Это делает защиту информации более важной, чем когда-либо ранее.

Понятие утечки информации

В общем, понятие "утечки информации" означает несанкционированное распространение конфиденциальной информации, которое может произойти из-за умышленных или случайных действий работников, а также из-за недостаточной защищенности с точки зрения технологий. [1]. Конфиденциальная информация может быть скомпрометирована как умышленными, так и случайными действиями сотрудников, а также из-за недостаточной технической защищенности. Незаконное получение или передача защищенных данных может привести к серьезным последствиям.

Среди наиболее распространенных причин утечки корпоративной информации можно выделить следующие:

– непреднамеренное или небрежное раскрытие данных, вызванное потерей конфиденциальной информации сотрудниками в общественных местах, предоставлением открытого доступа к данным в интернете или несоблюдением политики безопасности организации;

– инсайдерские угрозы, когда злоумышленник, получивший привилегированную учетную запись пользователя, злоупотребляет своими правами доступа и пытается вывести данные за пределы организации;

– угрозы внешних злоумышленников, целью которых являются конфиденциальные данные. Злоумышленники проникают через защитный периметр, используя такие методы, как фишинг, вредоносное программное обеспечение или внедрение кода, и получают доступ к конфиденциальной информации.

Традиционные методы защиты информации, вроде систем контроля и управления доступом, антивирусов и межсетевых экранов, не всегда могут предотвратить внутренние угрозы. Но существует решение для проблемы утечки конфиденциальных данных - DLP-системы. Это программное обеспечение позволяет отслеживать перемещение корпоративных данных, анализировать трафик и блокировать файлы в соответствии с политикой информационной безопасности организации.

DLP-решения помогают выявлять, контролировать, защищать и снижать риски утечки конфиденциальных данных. Они используются для предотвращения несанкционированного доступа к конфиденциальным данным и защиты информации, которая может быть передана третьим лицам по ошибке или намеренно [2].

Системы защиты от утечек конфиденциальной информации помогают предотвратить случаи несанкционированной передачи данных за пределы корпоративной сети. Кроме того, они могут отслеживать действия пользователей и анализировать их коммуникации через e-mail, социальные сети, чаты и другие каналы связи. Главная цель таких систем - обеспечить соблюдение политики конфиденциальности, установленной в организации.

Использование DLP-системы является актуальным для организаций, которые ценят конфиденциальность своих данных и боятся возможной утечки, приводящей к серьезным финансовым или репутационным проблемам. Также это решение подходит для компаний, которые строго следят за лояльностью своих сотрудников.

DLP-системы обеспечивают надежную защиту конфиденциальной информации, включая условия тендеров, заказы на услуги, номера пластиковых карт, данные о счетах клиентов, персональные данные сотрудников и клиентов, финансовые данные и многое другое. Это позволяет избежать потенциальных угроз и сохранить ценные данные в безопасности.

DLP-системы используются для фильтрации контента при отправке за пределы организации или в облачное хранилище. Они включают центр управления и мониторинга, агенты на рабочих станциях пользователей и сетевой шлюз DLP, который устанавливается на Internet-периметр. В зависимости от архитектуры подсистемы контроля, DLP-системы могут быть сетевыми, агентскими или гибридными.

Каждое из решений имеет свои преимущества и недостатки, поэтому выбор оптимальной DLP-системы должен основываться на ее способности предотвратить утечку информации по максимальному числу каналов передачи данных, используемых в организации.

DLP-решения предоставляют несколько функций, которые помогают обеспечить безопасность данных: мониторинг, фильтрация потоков данных, отчеты и анализ. Мониторинг обеспечивает видимость данных и доступ к системе, фильтрация потоков данных ограничивает подозрительную или неизвестную активность, отчеты полезны для ведения журнала и реагирования на инциденты, а анализ может выявлять уязвимости и подозрительное поведение. Применение подобных решений позволяет предотвращать утечки и несанкционированную передачу конфиденциальной информации, минимизировать риски финансового и репутационного ущерба, повышать дисциплину сотрудников, обеспечивать материал для расследования инцидентов и их последствий, а также ликвидировать угрозы безопасности информации, включая персональные данные. Все это позволяет обеспечить безопасность данных и улучшить работу компании.

Применение подобных решений имеет множество преимуществ. Во-первых, они предотвращают утечки и несанкционированную передачу конфиденциальной информации, что существенно снижает риски финансового и репутационного ущерба. Во-вторых, такие решения повышают дисциплину работников и создают материал для расследования инцидентов и их последствий. В-третьих, они ликвидируют угрозы безопасности информации, включая персональные данные, что соответствует требованиям по защите персональных данных.

В целом, использование подобных решений является необходимым шагом для обеспечения безопасности информации в современном мире. Однако, не следует забывать, что их применение должно быть интегрировано в повседневную работу компании и не вызывать дискомфорта у сотрудников. [4].

Как действовать при внедрении DLP-систем?

При внедрении DLP-системы в информационную систему организации необходимо тщательно настроить политику безопасности, чтобы защитить конфиденциальную информацию и соблюсти законодательство. На рынке информационной безопасности представлено множество DLP-систем, которые могут контролировать нелояльность сотрудников, пересылку информации из бизнес-приложений, печать и копирование бумажных документов, а также расследовать нарушения политики безопасности. Для достижения конкретных бизнес-целей используются различные инструменты, входящие в состав DLP-систем. Важно подобрать подходящую DLP-систему, чтобы эффективно защитить информацию и избежать неприятных последствий.

Внедряя DLP-систему в информационную систему организации необходимо проинформировать сотрудников о том, как это поможет предотвратить утечки конфиденциальной информации и представляет собой меру профилактики [3]. Также важно включить в политику безопасности организации запрет на использование корпоративной почты в личных целях, чтобы работники осознавали свою ответственность за использование почты и ее содержимого, которые являются собственностью организации [2].

Такие изменения не должны вызывать сильных эмоций и быть частью повседневной работы.

DLP-системы представляют собой инновационные решения, которые позволяют не только выявлять настроения в коллективе, но и контролировать нелояльных сотрудников еще на ранних этапах. Они используют лингвистический анализ и скрытый контекст сообщений для анализа подозрительной переписки. Также DLP-системы позволяют включить в группу риска категории работников, такие как находящиеся на испытательном сроке, планирующие уволиться или ранее нарушавшие политику безопасности.

Для идентификации DLP-системы используют три метода: вероятностный, детерминистский и комбинированный. Системы, основанные на первом методе, просты в реализации, но могут давать ложные срабатывания. Системы, использующие детерминированный подход, очень надежны, но не очень гибки. Комбинированный подход сочетает оба метода с аудитом среды хранения и обработки данных, что дает возможность достичь оптимального решения проблемы защиты конфиденциальности информации.

Существуют два основных подхода для анализа контента в программных решениях: фильтрация контента и контекстная фильтрация. Фильтрация контента основана на содержательном наполнении информации, а контекстная фильтрация использует принципиально другую схему: система проверяет контекст, в котором передается информация.

В целом, DLP-системы предоставляют эффективные решения для защиты конфиденциальной информации и контроля нелояльных сотрудников. Они особенно востребованы в компаниях, которые подвержены требованиям регуляторов, для которых утечка конфиденциальной информации является критической угрозой. В таких случаях, нарушение безопасности данных может привести к серьезным финансовым и репутационным рискам.

Вывод

DLP-системы - это программное обеспечение, которое может классифицировать конфиденциальную информацию, выявлять и предотвращать нарушения политики информационной безопасности, установленной организацией. Они являются эффективным инструментом для обучения и контроля за действиями сотрудников, а также защиты от непреднамеренных ошибок, мошенничества, вредительства и других противоправных действий. Кроме того, DLP-системы являются одним из способов управления корпоративными рисками.

Использование таких решений позволяет не только соблюдать обязательные меры по обеспечению информационной безопасности организации, но и предотвращать несанкционированное распространение конфиденциальной информации. Для решения конкретных бизнес-задач используются различные инструменты, входящие в состав данных систем. Существует тенденция к трансформации DLP-решений в системы защиты от более широкого спектра угроз. Это следующий этап их эволюции, согласно мнению экспертов.

Таким образом, использование DLP-систем является необходимым условием для обеспечения безопасности информации в организации и предотвращения возможных угроз.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Национальный стандарт РФ ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 декабря 2008 г. №532-ст). https://base.garant.ru/57969710/

2. Баранов, А. С. Использование систем предотвращения утечек данных в организациях / А. С. Баранов. — Текст: непосредственный // Молодой ученый. — 2020. — № 48 (338). — С. 15-16.

3. Мавринская Т. В. DLP-системы и тайна личных переписок / Т. В. Мавринская, А. В. Лошкарёв, Е. Н. Чуракова. — Текст: непосредственный // Интерактивная наука. — 2017. — № 4(14). — С. 181–183.

4. Программно-аппаратные средства защиты информационных систем: учебное пособие / Ю. Ю. Громов, Иванова О. Г., К. В. Стародубов, А. А. Кадыков. — Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017. — 193 с.

REFERENCES

1. The national standard of the Russian Federation GOST R 53114-2008 "Information protection. Ensuring information security in the organization. Basic terms and definitions" (approved by the Order of the Federal Agency for Technical Regulation and Metrology dated December 18, 2008 No. 532-st). https://base.garant.ru/57969710/

2. Baranov, A. S. The use of data leakage prevention systems in organizations / A. S. Baranov. — Text: direct // Young scientist. — 2020. — № 48 (338). — Pp. 15-16.

3. Mavrinskaya T. V. DLP-systems and the secret of personal correspondence / T. V. Mavrinskaya, A.V. Loshkarev, E. N. Churakova. — Text: direct // Interactive science. — 2017. — № 4(14). — Pp. 181-183.

4. Software and hardware protection of information systems: textbook / Yu. Yu. Gromov, Ivanova O. G., K. V. Starodubov, A. A. Kadykov. — Tambov: Tambov State Technical University, EBS DIA, 2017. — 193 p.

Информация об авторах

Донец Роман Юрьевич – Студент 1-го курса магистратуры по специальности Информационная безопасность. Безопасность информационных систем и технологий, Иркутский государственный университет путей сообщения, г. Иркутск, e-mail: donec_ryu@irgups.ru

Глухов Николай Иванович - канд. экон. наук, доцент каф. информационных систем и защиты информации, Иркутский государственный университет путей сообщения, г. Иркутск e-mail: gluhov_ni@irgups.ru

Information about the authors

Donets Roman Yurievich is a 1st–year Master's student in the specialty Information Security. Security of information systems and technologies, Irkutsk State Transport University, Irkutsk, e-mail: donec_ryu@irgups.ru

Glukhov Nikolay Ivanovich Candidate of Economic Sciences, Associate Professor of the Department of Information Systems and Information Protection, Irkutsk State Transport University, Irkutsk e-mail: gluhov_ni@irgups.ru