УДК 004.04

Предотвращение утечек конфиденциальной информации дизайн-студии технологиями DLP

Е.Ю. Потреба[*1], Н.Е. Губенко[*2]

[*1] магистрант, Донецкий национальный технический университет,
potrebart@gmail.com

[*2] к.т.н., доцент, Донецкий национальный технический университет,
negubenko@mail.ru

Потреба Е.Ю., Губенко Н.Е. Предотвращение утечек конфиденциальной информации дизайн-студии технологиями DLP. *В статье описывается проблематика возникновения инцидентов информационной безопасности. Актуализируется проблема утечки конфиденциальной информации. Приводится модель инфологической схемы для визуализации потоков обмена данными дизайн-студии. Рассматривается процесс внедрения технологий Data Leak Prevention в систему управления компанией. Анализируется функционирование системы для разграничения доступа в зависимости от занимаемых должностей сотрудников дизайн-студии. Затрагивается вопрос необходимости использования криптографической защиты данных в системе управления.*

Ключевые слова: *информационная безопасность, конфиденциальность, утечка данных, DLP-система, дизайн-студия, криптография*

Введение

Сложившаяся экономическая ситуация значительно усилила конкурентную борьбу компаний за позиции на рынке, а иногда и за выживание. 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.

Аналитики компании Falcongaze, утверждают, что половину 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. [1]

Стоит отметить, что деятельность дизайн-студий всегда была связана с обработкой и хранением большого количества конфиденциальных данных. Рабочий процесс дизайн-студии осуществляется посредством системы, в которой обрабатывается и хранится информация о текущих и реализованных проектах, о сотрудниках и их занятости, о персональных данных заказчиков.

Для предотвращения инцидентов информационной безопасности критически важно внедрить в систему управления дизайн-студией DLP-технологии (Data Leak Prevention), которые позволят анализировать перемещение данных, как внутри корпоративной сети, так и за её пределы, предотвращая утечку важной информации, согласно установленным правилам и политикам.

Целью статьи является актуализация вопросов безопасности конфиденциальных данных в информационных системах и внедрение технологий для минимизации соответствующих инцидентов.

Система управления дизайн-студией

Дизайн-студия — это организация, занимающаяся созданием веб-сайтов и фирменных стилей, отличительными особенностями которой является одновременное ведение нескольких проектов и постоянный контакт с различными заказчиками для уточнения, согласования и расчетов по заказанным услугам.

В состав организационной структуры рассматриваемой дизайн-студии входят сотрудники следующих должностей: арт-директор, проджект-менеджер, маркетолог, программист, дизайнер, бухгалтер, юрист, системный администратор. Предприятие оперирует огромными объемами данных: как результатами работы сотрудников, так и отчетностью и статистикой.

Программным образом система реализуется языком разработки веб-приложений PHP, веб-фреймворком Laravel, реляционной системой управления базами данных MySQL и программным стеком WAMP.

Для визуализации потоков обмена данными внутри системы спроектирована инфологическая модель. Она

представляет собой ориентированную на человека и не зависимую от типа СУБД модель предметной области, определяющую совокупности информационных объектов, их атрибутов и отношений между объектами, динамику изменений, а также характер информационных потребностей. [2]

Инфологическая схема дизайн-студии приведена на рис. 1:

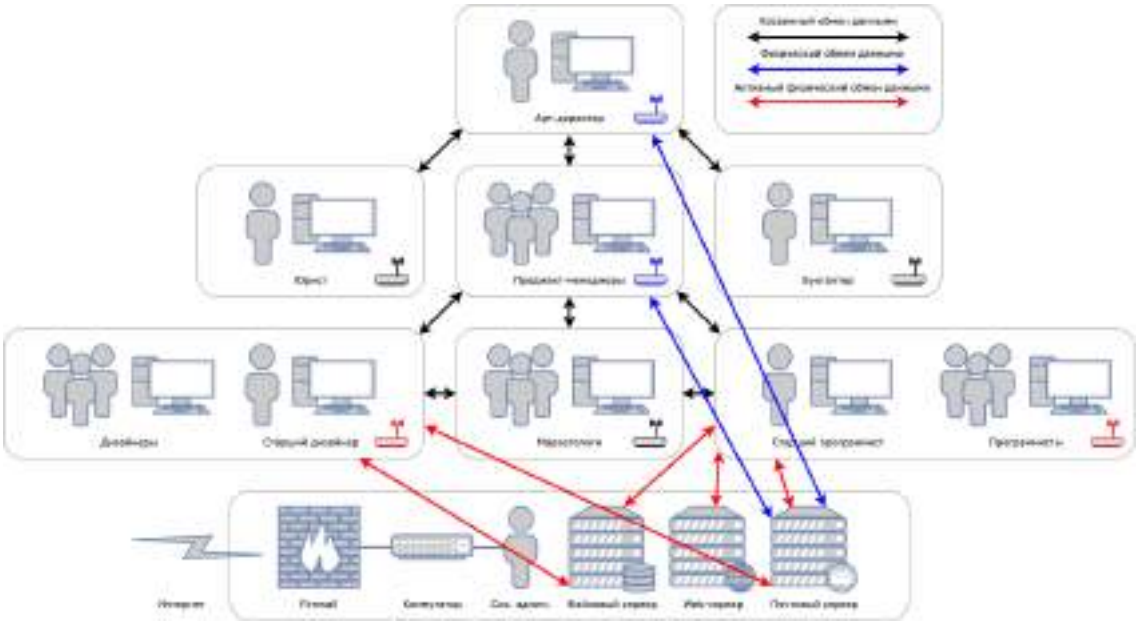

Рисунок 1 – Инфологическая схема дизайн-студии

На представленной инфологической схеме показаны потоки информации между участниками информационных процессов. На физическом уровне веб-сервер, файловый и почтовый сервер соединены с Интернетом через защищенный фаерволлом канал связи. Далее с помощью беспроводных точек доступа по локальной сети разные отделы обращаются к серверам.

Большое количество сотрудников и объем связей разных типов обмена данных повышают вероятность появления угроз конфиденциальности информационных ресурсов.

Угрозы конфиденциальности информационных ресурсов

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;

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.

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 документа и путём анализа 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, медиа-контента).

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).

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. [4]

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 и описать, как использование системы защиты информации способствует финансовому благополучию компании. Отдельно стоит подчеркнуть, что руководитель дизайн-студии имеет право на защиту коммерческой тайны организации, а компьютеры и другая техника, которую предоставляет работнику, являются собственностью компании, и для защиты собственности может применяться любая система защиты. [5]

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.

Внедрение DLP-технологий в систему управления дизайн-студией

Перед процессом внедрения DLP важно провести подготовительные процедуры. Процесс подготовки компании к установке системы защиты состоит из аудита защищенности информации, оценки рисков и урегулирования юридических вопросов. Аудит подразумевает оценку реальной степени защиты информации. На этом подготовительном отрезке идет поиск возможных каналов уязвимостей в данной экосистеме.

Помимо этого, в рамках внедрения DLP-технологий в систему управления дизайн-студией необходимо провести обследование информационных потоков, которое включает:

1. Оценку уровня безопасности при работе с внутренними документами компании.
2. Детальное изучение всех технических ресурсов компании, от серверов до сетевых потоков.
3. Создание перечня данных, которые относятся к группе информации с ограниченным доступом.
4. Разработка правил разграничения доступа.
5. Изучение процессов обработки, создания, передачи и хранения информации в рамках компании.

Оценка риска и создание правил разграничения доступа – обязательные шаги на этапе внедрения экономически эффективной DLP-системы. Риски оцениваются наряду с обследованием потенциальных каналов утечки. В зависимости от вероятного ущерб принимается решение о необходимости защиты канала утечки. [6]

Таким образом, опишем функционирование системы управления дизайн студией для создания правил разграничения доступа – набора прав, которые получает пользователь системы в зависимости от занимаемой должности. На рис. 2 изображена диаграмма вариантов использования разрабатываемой системы, которая включает в себя функции доступные администратору, сотрудникам и клиентам дизайн-студии:

Функции, доступные администратору: добавление сотрудников, назначение сотрудников, изменение данных о сотруднике, изменение этапа разработки, просмотр данных о заказе, заполнение брифа, добавление проекта, изменение данных о клиенте.

Функции, доступные клиенту: изменение данных о клиенте, заполнение брифа, просмотр данных о заказе.

Функции, доступные сотруднику: изменение данных о сотруднике, изменение этапа разработки, просмотр данных о заказе.

Рисунок 2 – Диаграмма вариантов использования

Чтобы предотвратить возможность несанкционированного доступа к конфиденциальной информации, решено использовать отдельные личные кабинеты для реализации разделения прав пользователей системы.

В свою очередь, для обеспечения безопасности всей системы, особое внимание необходимо уделить вопросу надежного хранения и шифрования аутентификационных данных от созданных личных кабинетов пользователей. Для предотвращения рисков, связанных с утечкой данных и обеспечения информационной безопасности общества, прежде всего, применяются методы криптографической защиты посредством шифрования данных.

В рамках защиты конфиденциальной информации дизайн-студии должен использоваться криптостойкий алгоритм с высокой скоростью шифрации и дешифрации (за счет генерации таблиц замены).

Стоит отметить, что для дизайн-студии, где безопасность данных входит в число бизнес-приоритетов, внедрение DLP – оптимальный выбор. Успешная интеграция DLP позволит контролировать все потоки информации, а также вовремя выявлять и устранять угрозы безопасности.

Выводы

В статье описана проблематика возникновения инцидентов информационной безопасности. Актуализирована проблема утечки конфиденциальной информации. Приведена разработанная инфологическая схема для визуализации потоков обмена данными дизайн-студии. Рассматривается процесс внедрения технологий Data Leak Prevention в систему управления компанией. Проанализировано функционирование системы для разграничения доступа в зависимости от занимаемых должностей сотрудников дизайн-студии. Затронут вопрос необходимости использования криптографической защиты персональных данных в системе управления. Подчеркнута важность проведения дальнейших работ для комплексного обеспечения информационной безопасности дизайн-студии.

Литература

1. DLP-системы — элемент информационной безопасности [Электронный ресурс]. Режим доступа: https://www.azone-it.ru/dlp-sistemy-vazhnaya-sostavlyayushchaya-informacionnoy-bezopasnosti-predpriyatiya – Загл. с экрана.

2. Инфологическая модель предметной области [Электронный ресурс]. Режим доступа: https://studbooks.net/2278354/informatika/infologicheskaya_ model_predmetnoy_oblasti – Загл. с экрана.

3. Основы информационной безопсности [Электронный ресурс]. Режим доступа: https://цбис.рф/osnovy-informatsionnoj-bezopasnosti – Загл. с экрана.

4. Информационная безопасность. Защита данных с помощью DLP-системы [Электронный ресурс]. Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy – Загл. с экрана.

5. Внедрение DLP-системы на предприятии [Электронный ресурс]. Режим доступа: https://spravochnick.ru/informatika/vnedrenie_dlp-sistemy_na_predpriyatii – Загл. с экрана.

6. Информационная безопасность. Внедрение DLP-систем [Электронный ресурс]. Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/dlp-sistemy/vnedrenie-dlp-sistem – Загл. с экрана.

Потреба Е.Ю., Губенко Н.Е. Предотвращение утечек конфиденциальной информации дизайн-студии технологиями DLP. *В статье описывается проблематика возникновения инцидентов информационной безопасности. Актуализируется проблема утечки конфиденциальной информации. Приводится модель инфологической схемы для визуализации потоков обмена данными дизайн-студии. Рассматривается процесс внедрения технологий Data Leak Prevention в систему управления компанией. Анализируется функционирование системы для разграничения доступа в зависимости от занимаемых должностей сотрудников дизайн-студии. Затрагивается вопрос необходимости использования криптографической защиты данных в системе управления.*

Ключевые слова: *информационная безопасность, конфиденциальность, утечка данных, DLP-система, дизайн-студия, криптография*

Potreba Efim, Gubenko Natalia Prevention of leaks of confidential information of a design studio by DLP technologies. *The article describes the problems of information security incidents. The problem of leakage of confidential information is being updated. The model of the infological scheme for visualization of data exchange flows of the design studio is given. The process of implementing Data Leak Prevention technologies into the company's management system is considered. The functioning of the system for access differentiation is analyzed depending on the positions held by design studio employees. The issue of cryptographic protection of personal data in the management system is touched.*

Keywords: *information security, confidentiality, data leakage, DLP system, design studio, cryptography*