**ISSN 2225-6741. Рынок транспортных услуг
(проблемы повышения эффективности).
Вып. 17. Гомель, 2024**

УДК 004.56:656.2(476)

И. А. БОВА
Гомельский государственный университет им. Ф. Скорины

СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНИЗАЦИЯХ БЕЛОРУССКОЙ ЖЕЛЕЗНОЙ ДОРОГИ

Рассматриваются основные аспекты управления информационной безопасностью в организациях Белорусской железной дороги и направления их совершенствования. Особое внимание уделено DLP-системам, которые помогают защищать данные от утечек, соблюдать законодательство в сфере информационной безопасности, повышать эффективность бизнеса.

Белорусская железная дорога, являясь одной их стратегических отраслей, применяет современные информационные технологии в различных сферах своей деятельности: при организации управления движением поездов, при организации и осуществлении пассажирских перевозок, при обработке различной управленческой, финансовой и бухгалтерской информации и т. п. В связи с чем особую актуальность приобретает обеспечение информационной безопасности для защиты от информационных атак и рисков.

Основные виды информационных рисков в разрезе объектов воздействия обобщим в таблице 1.

Таблица 1 **– Виды информационных рисков в разрезе объектов воздействия**

Вид информационного риска	Объект воздействия риска		
	Оборудование	Программное обеспечение	Данные
Утечка конфиденциальной информации	Несанкционированное подключение к каналам связи, хищение носителей информации	Несанкционированное копирование и перехват информации	Хищение, копирование, перехват
Потеря важных данных	Несанкционированное использование ресурсов; подключение, модификация, изменение режима работы	Внедрение вредоносных файлов	Искажение, модификация
Нарушение целостности информации	Хищение, разрушение, нарушение работы	Изменение и уничтожение	Изменение, уничтожение

Окончание таблицы 1

Вид информационного риска	Объект воздействия риска		
	Оборудование	Программное обеспечение	Данные
Распространение заведомо ложной информации в средствах массовой информации	Производство нелицензионных копий продукции	Использование нелицензионных копий	Использование материалов без разрешения автора

По механизму воздействия информационные риски можно разделить следующим образом:

– выход из строя технического и сетевого оборудования;

– просчеты и упущения системных администраторов;

– нарушение работы программного обеспечения;

– использование вредоносных программ;

– внедрение следящего шпионского оборудования;

– нарушение режима тайны;

– нарушение лицензионных прав;

– распространение дискредитирующей информации [1].

Минимизация последствий рисков информационной безопасности предполагает использование методов управления рисками. Для эффективного управления информационной безопасностью на Белорусской железной дороге, по мнению автора, целесообразно:

– обеспечить разработку и реализацию политики информационной безопасности;

– разработать нормативно-методические документы обеспечения информационной безопасности;

– создать административное и кадровое обеспечение комплекса средств управления информационной безопасностью;

– осуществлять мониторинг функционирования системы информационной безопасности;

– совершенствовать программное обеспечение и повышать квалификацию персонала организации в области информационной безопасности;

– управлять рисками, связанными с нарушением информационной безопасности.

В настоящее время необходимым и актуальным инструментом обеспечения информационной безопасности бизнеса являются DLP-системы. Они помогают организациям защищать данные от утечек, соблюдать законодательство в сфере информационной безопасности, повышать конкурентоспособность и эффективность деятельности.

Учитывая специфику деятельности Белорусской железной дороги, на наш взгляд, наиболее подходящим программным продуктом для минимизации

последствий рисков информационной безопасности является DLP-система *InfoWatch Traffic Monitor* от признанного лидера в сфере защиты корпоративных данных на рынке России и стран СНГ компании *InfoWatch* [2].

Вышеназванная DLP-система обладает следующим функционалом:

– дает возможность обнаружить мошенничество и сговоры внутри компании;

– помогает контролировать деятельность сотрудников и определять их степень лояльности к политике компании;

– предотвращает неправомерные действия сотрудников (распространение нежелательной информации, распространение сведений ограниченного доступа);

– дает возможность сформировать доказательную базу для проведения внутренних расследований инцидентов информационной безопасности.

Здесь следует подчеркнуть, что основные функции обеспечения информационной безопасности Белорусской железной дороги реализуются внутренними подразделениями информатизации (вычислительными центрами, отделами управления и поддержания информационной инфраструктуры). Зачастую специалисты вышеуказанных подразделений пытаются скрыть или замаскировать все сбои и отказы сетевого и программного оборудования. Это сказывается на качестве анализа причин и проведения расследований указанных инцидентов.

В системе InfoWatch Traffic Monitor предусмотрены следующие технологии инспекции трафика:

– детектирование скачиваний из баз данных (ведомости заработных плат работников, отчеты о прибылях и убытках, индивидуальные данные сотрудников и др.);

– классификация информационных потоков по категориям (лингвистический анализ);

– детектирование текстов по установленным шаблонам;

– детектирование фрагментов текста, относящихся к эталонным документам;

– детектирование заполненных бланков по установленным шаблонам (резюме, лицевые счета, платежные документы и т. д.);

– детектирование сканированных копий паспортов;

– детектирование печатей по установленным образцам;

– детектирование изображений по установленным шаблонам (паспорт, платежная карта и т. д.);

– контроль процессов печати и сканирования документов, передвижения отсканированных копий;

– мониторинг файлов в соответствии с заданным форматом файлов.

Рассмотрим список действий по развертыванию системы *InfoWatch Traffic Monitor*:

– подготовка всех компонентов к внедрению – выбор аппаратных составляющих, подготовка рабочих станций пользователей, резервное копирование конфигураций;

– инсталляция компонентов *InfoWatch Traffic Monitor* на сервер безопасности;

– предварительная настройка политики безопасности и политики мониторинга трафика;

– установка компонента *InfoWatch Device Monitor* на пользовательские рабочие места;

– сетевое подключение сервера безопасности *InfoWatch*, наладка процессов взаимодействия пользователей;

– тестирование и эксплуатация системы;

– промышленная эксплуатация системы и анализ сбоев и нарушений в работе.

Для обеспечения нейтрализации актуальных угроз информационной безопасности в системе *InfoWatch Device Monitor* могут выбираться следующие сценарии работы:

1 Блокировка утечек конфиденциальной информации. При реализации данного сценария происходит блокировка передачи данных с рабочих компьютеров сотрудников при обнаружении в них конфиденциальных данных. Блокировка передачи файла происходит и при попытке копирования контролируемых файлов на носители. Служба безопасности получает сообщения о нарушении политики безопасности, события фиксируются в журнале и являются доступными для ознакомления.

2 Запрет операций при работе в бизнес-приложениях. Дает возможность формировать правила на запрет исполнения отдельных действий по защищенным документам и файлам: копирование, печать и снятие скриншотов. Такой запрет позволяет вести контроль приложений, которые не учитывают разграничения прав для конкретных операций.

3 Предотвращение утечек информации из баз данных. Сведения о потребителях продуктов и услуг, контрагентах, партнерах, составленные в разных базах, являются основной конфиденциальной информацией. В *InfoWatch Traffic Monitor* для выявления утечек из таких баз формируется эталонный отпечаток базы. Система детектирует каждое сообщение (письмо, публикацию, файл), сопоставляет выявленные текстовые фрагменты с данными из эталонного отпечатка. Если система находит совпадение, сетевой администратор получает соответствующее уведомление об инциденте.

4 Защита объектов интеллектуальной собственности. Такая защита подходит для разработок, которые уже окончательно оформлены и доработаны. При реализации указанного сценария *InfoWatch Traffic Monitor* применяет разные своды правил обработки информации: базы контентной фильтрации, представляющие собой иерархический список категорий из слов и формули-

ровок, позволяющих установить тематический смысл и соответствующий уровень конфиденциальности данных.

Обобщая вышесказанное, отметим, что внедрение DLP-системы InfoWatch Traffic Monitor позволит Белорусской железной дороге обеспечить с точки зрения информационной безопасности:

– детектирование попыток нарушения информационной безопасности со стороны внутренних пользователей;

– минимизацию рисков утечки конфиденциальных данных;

– мониторинг соблюдения режима конфиденциальности и политики информационной безопасности;

– контроль доступа к определенным информационным активам;

– архивирование сообщений о нарушениях информационной безопасности с целью проведения компетентных служебных расследований;

– соблюдение норм законодательных актов в части информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ

1 **Петренко, С. А.** Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : Компания «Аути» : ДМК «Пресс», 2024. – 384 с.

2 Компания «InfoWatch» : [офиц. сайт]. – М., 2003–2024. – URL : https://www. infowatch.ru/ products/dlp-sistema-traffic-monitor (дата обращения : 16.08.2024).

3 **Шатров, С. Л.** Теория и методология информационно-аналитического обеспечения системы управления внешнеэкономической деятельностью на железнодорожном транспорте : [монография] / С. Л. Шатров. – Гомель : БелГУТ, 2018. – 232 с.

I. BOVA
Gomel State University named after Francisk Scorina

IMPROVING THE INFORMATION SYSTEM SECURITY IN THE ORGANIZATIONS OF THE BELARUSIAN RAILWAY

The article discusses the main aspects of information security management in the organizations of the Belarusian Railway and the directions for their improvement. Particular attention is paid to DLP systems that help protect data from leaks, comply with information security legislation, and increase business efficiency.

Получено 07.10.2024