Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет

информатики и радиоэлектроники»

УДК658.29-049.5

Пузына

Сергей Викторович

«Методика защиты конфиденциальной информации банков на основе DLP-систем»

АВТОРЕФЕРАТ

на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель

Маликов Владимир Викторович

кандидат технических наук, доцент

Минск, 2015

ВВЕДЕНИЕ. ПОСТАНОВКА ЗАДАЧИ

Конфиденциальная информация является критически важным объектом любой организации, а ее утечка может привести к возникновению серьезных репутационных (когда сам факт утечки может повлиять на имидж компании), юридических (например, нарушение законодательства о персональных данных) и прямых финансовых рисков компании. Внедрение DLP-системы позволяет снизить такие риски, путем предотвращения утечки информации, и обеспечить доказательную базу при проведении расследований инцидентов, связанных с утечкой конфиденциальной информации. Объектом исследования является структура получения, обработки и хранения конфиденциальной информации в банках, а также организационно-технические подходы для совершения преступлений со стороны криминальных организаторов. Предметом исследования являются организационно-технические и технические методы защиты на основе DLP-систем, способствующие повышению эффективности защиты конфиденциальной информации банков.

В диссертационной работе ставятся и решаются задачи исследования и разработки методики защиты конфиденциальной информации банков на основе DLP-систем. Полученные аналитические соотношения охватывают многопозиционные виды модуляции и помехоустойчивое свёрточное кодирование.

БАЗОВЫЕ ПОЛОЖЕНИЯ, ВЫНОСИМЫЕ НА ЗАЩИТУ

Во введении обосновывается актуальность выбранной темы, даётся краткая характеристика её разработанности, определяются объект и предмет исследования, цель и задачи, формулируются основные положения диссертации, выносимые на защиту.

Первый раздел «Статистические данные по утечкам конфиденциальной информации банков»носит теоретический характер и состоит из двухподразделов.

В подразделе 1.1. «Угрозы безопасности конфиденциальной информации» выделены два существенных вопроса. Первый – статистические данные по нарушению систем защиты. Анализ угроз, проведенных агентством национальной ассоциацией информационной безопасностив США выявил следующую статистику: 43% угроз – сбои оборудования, 26% - неумелые или неправильные действия персонала, 15% - вредительские действия собственных сотрудников, 8% - внешние атаки по сети Интернет и 5% - воздействие

компьютерных вирусов. Классификация угроз информационной безопасностиявляется вторым вопросом и рассматривается в подразделе 1.1.2.Все источники угроз безопасности информации можно разделить на три основные группы: обусловленные действиями субъекта (антропогенные источники угроз); обусловленные техническими средствами (техногенные источники угрозы); обусловленные стихийными источниками.

В подразделе 1.2. «Статистические данные по методам и средствам обеспечения безопасности конфиденциальной информации» рассматриваются организационно-технические и технические средства защиты информации. Рассмотрены уровни защиты: законодательный, административный, процедурный и программно-технический. Приведены аппаратные и программные средства защиты информации.

Основные направления исследований по повышению эффективности защиты конфиденциальной информации банков на основе DLP-систем рассмотрены в подразделе 1.3. Возможности современных систем DLP позволяют отслеживать и распознавать информационные потоки, при необходимости блокировать их, а также систематизировать и хранить передаваемую информацию с целью ее дальнейшего анализа и сбора доказательной базы.

Второй раздел «Оценка эффективности методов и средств защиты конфиденциальной информации банков на основе DLP-систем» состоит из трёх разделов, рассматривающих концептуальные основы построения систем защитына основе DLP-систем(подраздел 2.1), методические основы выбора и применения типовых DLP-систем (подраздел 2.2), а также подраздел, посвященный разработке подхода по оценке эффективности систем защиты на основе DLP-систем. В подразделе 2.1 рассмотрены традиционный и комплексный подходы к построению системы защиты от утечек КИ на основе DLP-системы. Традиционный подход идеален для «быстрого старта», мониторинга обработки заранее определенного конкретного пула защищаемой информации/документов. В рамках комплексного подхода производится системный анализ области (бизнес-процессы, прикладные области процессов, например процесс заключения договоров), формируются и внедряются процедуры инвентаризации, классификации и категорирования информации, расследования инцидентов. В подразделе 2.3 описаны этапы подготовки к внедрению системы, рассмотрена модель нарушителя безопасности, разработаны критерии эффективности систем защиты. Оценку эффективности можно производить по следующим критериям:1) количество ложных срабатываний или ложных тревог (ошибки первого рода);2) пропущенные

(необнаруженные) утечки информации (ошибки второго рода);3) трудоемкость (быстродействие) DLP-системы.

Третий раздел «Методика защиты конфиденциальной информации банков на основе DLP-систем» носит практико-ориентированный характер и состоит из трёх подразделов, рассматривающих статистические данные по утечкам (подраздел 3.1), оценку применимости существующих подходов для повышения эффективности защиты конфиденциальной информации банков(подраздел 3.2), а также включает разработку методики защиты (подраздел 3.3). В подразделе 3.2 рассмотрены способы защиты от наиболее распространённых способов воровства конфиденциальной информации:1) физический доступ к местам ее хранения и обработки; 2) использование резервных копий;3) несанкционированный доступ сотрудниками банка. В подразделе 3.3 рассмотрен пример модели преступления, а также возможные варианты решения. В основном для категоризации данных в продуктах по защите корпоративной информации от утечек используются две основных группы технологий — лингвистический (морфологический, семантический) анализ и статистические методы. Каждая технология имеет свои сильные и слабые стороны, которые определяют область их применения.Использование лингвистического подхода и подхода, основанного на цифровых отпечатках информации необходимо применять последовательно.

Цифровые отпечатки лучше справятся с определением типа документа — договор это или балансовая ведомость. Затем можно подключать уже лингвистическую базу, созданную специально для этой категории. Это сильно экономит вычислительные ресурсы.

В четвертом разделе «Автоматизация подходов по защите конфиденциальной информации банков на основе DLP-систем» рассмотрены основные принципиальные модули системы DLP, рассмотрена схема развертывания модулей DLPв инфраструктуре организации. Основное назначение DLP – обеспечивать защиту от случайного или намеренного распространения конфиденциальной информации со стороны сотрудников, имеющих доступ к информации в силу своих должностных обязанностей. Но, помимо того, любая DLP может быть настроена и для борьбы со злонамеренными инсайдерами. В подразделе 4.2 рассмотрены и проанализированы шесть наиболее популярных на рынке информационной безопасности DLP-систем по состоянию на конец2013 года. Все участники произвели благоприятное впечатление и могут использоваться для предотвращения утечек информации. Различия продуктов позволяют конкретизировать область их применения.

ЗАКЛЮЧЕНИЕ

Базируясь на проведенных в диссертационной работе теоретических исследованиях, касающихся методов защиты информации банков на основе DLP-систем, можно сделать вывод:

– проведен анализ статистических данных по утечкам конфиденциальной информации банков на основе которого показано, что основным каналом утечек информации является неудовлетворительное поведение и неудовлетворенное ожидание персонала, а также нерациональные способы хранения, передачи и обработки информации. Выявлено, что в первую очередь необходим контроль и анализ поведения сотрудников, собирающихся покинуть компанию (поиск работы или обсуждение полученных предложений) и негативно реагирующих на управленческие решения.;

– обосновано, что главной задачей при организации защиты и расследования инцидента информационной безопасности является поиск источника утечки информации;

–установлено, что для защиты конфиденциальной информации банков необходимо совместное применение организационно-технических и технических методов;

–при разработке методики по защите конфиденциальной информации банков на основе DLP-систем доказано, что оптимальным с точки зрения технической реализации защиты конфиденциальной информации банков на основе DLP-систем является последовательное использование комбинации лингвистического подхода и подхода, основанного на цифровых отпечатках информации.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

–Маликов, В.В. Исследование структуры и технологий совершения киберпреступлений / В.В. Маликов, Р.В. Рабцевич, С.В. Пузына // 50-лет МРТИ-БГУИР: материалы Международной НТК – Минск, 18-19 марта 2014 г.: в 24./БГУИР; редкол.: А.А. Кураев [и др.] – Мн., 2014. 4.1 – с.396-397