Информатика, вычислительная техника и управление

УДК 004.056.5
DOI: 10.30987/1999-8775-2020-6-38-49

В.И. Андрианов, Д.И. Сивков, Д.В. Юркин

МЕТОДИКА ВНЕДРЕНИЯ СИСТЕМЫ ПРЕДОТВРАЩЕНИЯ УТЕЧЕК ИНФОРМАЦИИ (*DLP*) В КОММЕРЧЕСКУЮ ОРГАНИЗАЦИЮ ДЛЯ ИНФОРМАЦИОННОЙ СЕТИ С ИСПОЛЬЗОВАНИЕМ БОЛЬШИХ ДАННЫХ

Исследуются основные достоинства и недостатки внедрения системы предотвращения утечек информации DLP в коммерческую организацию для информационной сети с использованием больших данных. Целью работы является создание методики, позволяющей специалистам информационной безопасности, а также руководителям, разобраться в работе DLP-системы. Проектная экспертиза внедрения системы предотвращения утечки информации в организацию, а как же предложения по реализации архитектуры с известными сигнатурами атак для выявления внутренних угроз сети.

Ключевые слова: DLP, утечка данных, защита, конфиденциальные сведения, обработка информации.

V.I. Andrianov, D.I. Sivkov, D.V. Yurkin

PROCEDURE FOR IMPLEMENTATION OF DATA LEAKAGE PREVENTION (*DLP*) SYSTEM TO COMMERCIAL COMPANY FOR INFORMATION NETWORK USING LARGE DATABASE

The purpose of this work consists in the creation of such a procedure according to which a head or an expert dealing with the information safety in a company could make a decision quickly, whether he has got to install a system for intrusion prevention or not, and also how to substantiate a leadership the necessity The environment constantly develops and changes due to new technologies and the Internet. The products of intrusion detection are tools which help to control threats and voidability in this changing environment. Threats are people or groups which can jeopardize your computer system. It may be an inquisitive teenager, a discontented worker or it may be espionage of a rival company or a foreign government. That is why the implementation of a data protection system against leakage is an urgent necessity for companies in the modern world.

The information content obtained for processing increases on a dynamic scale around the world. The information content incoming for processing grows on a dynamic scale all over the world. For the purpose of a quick reaction to any market changes, obtaining competitive advantages, increased production is required quick obtaining, processing and analyzing large data contents.

of costs for operation. On this reason, there are defined basic advantages and disadvantages of the installation of the DLP system and there is shown a design examination of an attempt to implement the system in a commercial company.

Key words: DLP, data leakage, protection, confidential information, information processing.

Введение

Основные задачи данной системы *DLP* (*Data Leak Prevention*): анализ передающейся конфиденциальной информации по всем каналам, таким как: электронная почта, *Web*-почта, *HTTP*-трафик, *IM*-сервисы, социальные сети, мессенджеры, облачные хранилища информации, а также *USB*-устройства, *CD/DVD*, локальная печать. Благодаря мониторингу происходит обнаружение случаев несанкционированной передачи конфиденциальных данных, блокирование, а также оповещение отдела службы безопасности об инцидентах.

Однако современные *DLP*-системы также вмещают в себя функции контроля действия персонала, выявление групп риска среди сотрудников и контроль настроений в коллективе, шифрование передаваемой информации, выявление мошенничества с возможностью проведения ретроспективных расследований и оценка эффективности и продуктивности пользователей [1,2].

Очевидно, что необходимо защищаться от внутренних угроз, но чаще всего приоритет отдавался защите от внешних нарушителей. В связи с федеральным законом 152 "О персональных данных" и федеральным законом 149 "Об информации, информационных технологиях и о защите информации" в настоящее время можно с уверенностью можно сказать, что внутренние источники угроз – сотрудники предприятий или другие лица, имеющее легальный доступ к данным.

Предмет исследования *DLP* и статистических данных о каналах утечки информации

Согласно глобальному исследованию утечек конфиденциальной информации аналитического центра *InfoWatch* в 2019 году, произошло 1276 случаев утечки конфиденциальной информации (рис. 1).

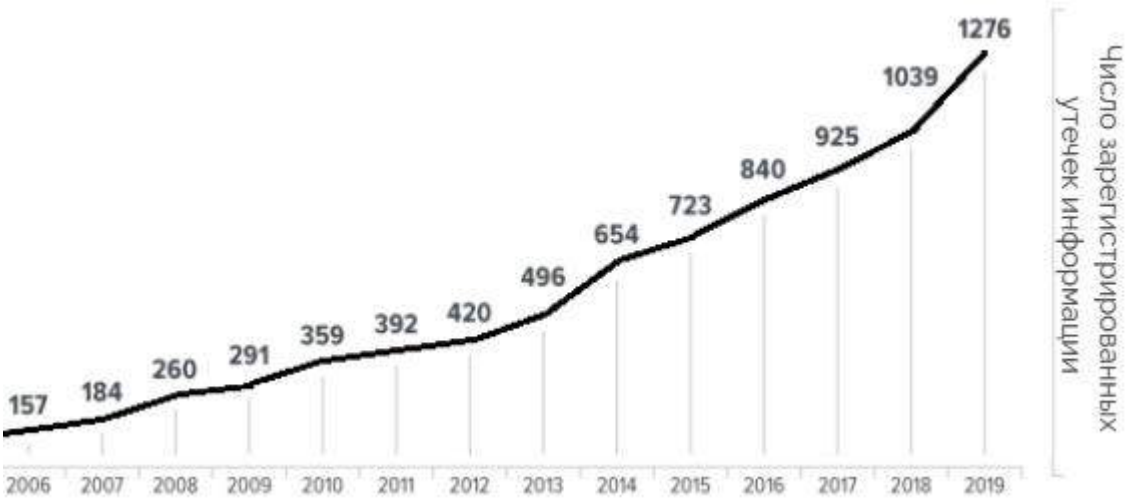

Рис. 1. Число зарегистрированных утечек информации 2006 - 2019

На рис. 2 можно увидеть, что внешние атаки стали причиной 44,4% утечек данных, а в остальных 55,6% случаев утечка данных произошла под воздействием внутреннего нарушителя.

Рис. 2. Распределение утечек по вектору воздействия за 2019 год

Следует отметить, что внутренние утечки информации по своей природе труднее предотвратить. Они имеют более сложный комплекс последствий, чем утечки из-за внешних нарушителей [3,4].

В 44,8% случаев виновниками утечек данных фактически были сотрудники компаний и 2,8% - бывшие сотрудники (рис. 3). По вине руководителя, системного администратора и подрядчика было зафиксировано всего 6,2% случаев утечки информации. Топ-менеджмент и непривилегированные сотрудники склонны к нарушению установленных правил безопасности. Это касается не только незаконного распространения информации ограниченного доступа, но и действий, которые прямо направлены на причинение ущерба работодателю и ведут к блокированию или уничтожению данных.

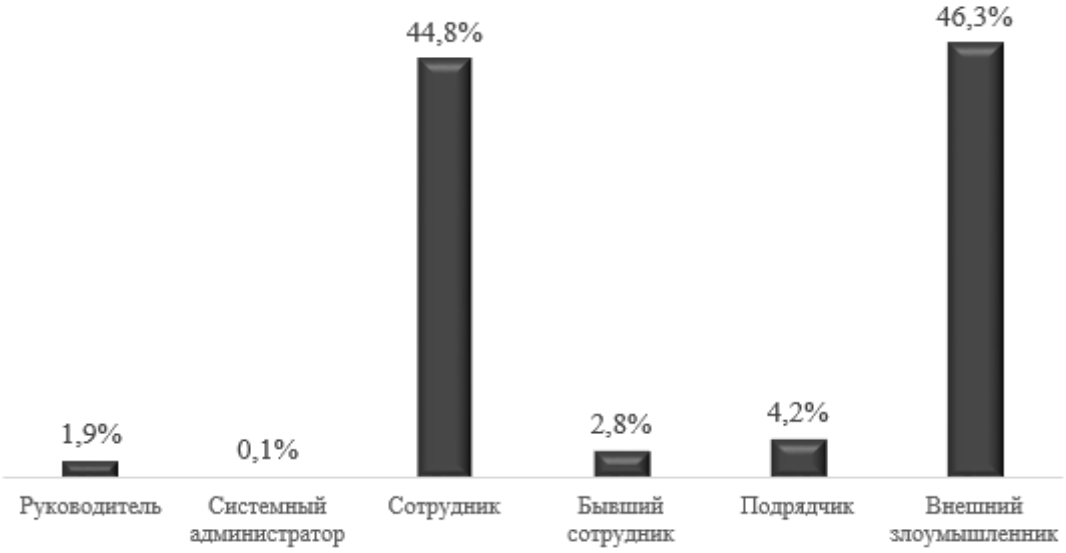

Рис. 3. распределение утечек по виновнику 2019 год

Наибольшее число умышленных утечек информации было через сеть 76,6 %, на втором месте через отправку по электронной почте 8,4%, третье место занимают бумажные носители 6,3%, остальные - съемные носители, мобильные устройства, кража или потеря оборудования (рис. 4). Системы мгновенного обмена сообщениями составляют всего 8,7%.

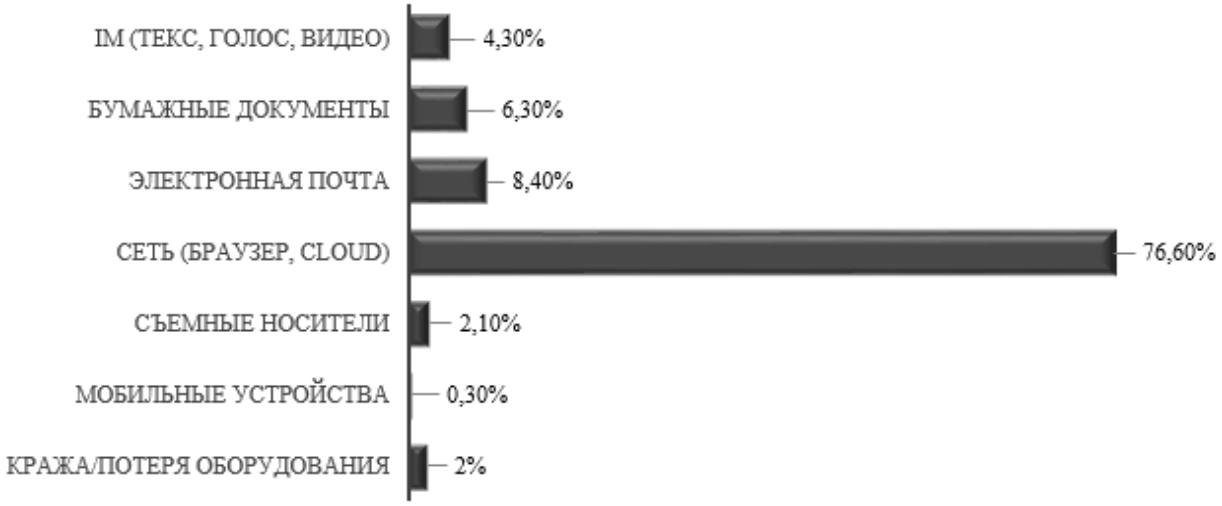

Рис. 4. Распределение утечек по каналам 2019 год

Все представленные данные получены из открытых источников. Распределения умышленных и случайных утечек справедливы только для инцидентов, которые фактически имели место (их не удалось предотвратить) и получили огласку (о них стало известно). Такая ситуация требует дополнительных разъяснений. С учетом сегодняшнего уровня развития технологий можно предположить, что зафиксированные на этих каналах утечки составляют лишь небольшую часть от числа случаев, когда информация уходила из-под контроля обладателей по этим каналам [5].

Известно, что многие системы защиты показывают невысокую эффективность на таких каналах перехвата утечек, как голосовая передача данных, мессенджеры, мобильные устройства. Кроме того, умышленные утечки в принципе сложнее предотвратить. Учитывая сказанное, авторы исследования полагают, что к небольшим значениям долей умышленных утечек через большинство каналов, за исключением сетевого, следует отнестись критически. Вопреки приведенному распределению, в силу перечисленных выше особенностей, каналы, на которых зафиксировано небольшое количество утечек, нуждаются в особом внимании со стороны служб безопасности. Здесь нужен целый комплекс решений, включая тщательно настроенные *DLP*-системы и инструменты контроля доступа. Отдельную роль в выявлении сотрудников, склонных к краже корпоративных данных, должны играть системы предиктивной аналитики.

Выявление основных преимуществ и недостатков внедрения *DLP*-системы в коммерческую организацию

Перед тем как внедрять систему мониторинга и предотвращения утечек информации важно понимать, какие конкретные задачи она будет решать и с чем бороться. Покажем важные аспекты при установке *DLP*-системы (табл. 1, 2).

Таблица 1

Недостатки внедрения DLP-системы

Недостаток	Описание
1. Высокая цена установки и поддержание работоспособности системы	Целесообразно внедрять *DLP*-систему в большие компании, где существует целый *IT*-отдел, связанный с безопасностью, где есть достаточное количество квалифицированных сотрудников, для анализа всех событий, а как же если существует угроза секретной и конфиденциальной информации, которую требуется защищать. Стоит учитывать, что стоимость внедрения таких систем высокая и иногда может превышать стоимость ущерба при утечке информации.
2. Есть возможность использования *DLP*-системы в корыстных целях	К сожалению, никто не застрахован от не добросовестных сотрудников, которые работают в *IT*-отделе и эксплуатируют *DLP*-систему. Они сами могут следить за всем персоналом, в том числе и за топ-менеджерами, руководителями отделом и даже самим директором незаметно для них. Тем самым возникает риск утечки информации через самих специалистов по информационной безопасности.
3. Долгий процесс полного внедрения	Пред тем как внедрить *DLP*-систему в организации следует предварительно выявить потенциальные каналы утечки информации, т.е. рабочие места, с которых могут быть похищены важные данные, определить круг лиц, владеющих конфиденциальной информацией. Это может выполнять, как специалист по информационной безопасности в компании, а также сама компания, которая внедряет *DLP*-систему. По итогам исследования формируется политика безопасности *DLP*-

Недостаток	Описание
	системы, которая будет содержать перечень информации ограниченного доступа, схему потоков данных информации ограниченного доступа, описание технологических процессов взаимодействия с информацией ограниченного доступа и основные сценарии утечки конфиденциальной информации. Далее важную частью внедрения системы занимает ее юридическое сопровождение. Тут решаются вопросы: “Будет ли считаться использование этой системы, как слежка за сотрудниками?”, или “Необходимо будет хранить все произошедшие события или только те, которые нарушили политику безопасности?”. Компания должна подготовиться, к потенциальному спору с сотрудником, из-за внедрения такой системы. После установки *DLP*-системы в организации, последним этапом необходимо будет ее правильно настроить, чтобы она работала должным образом. Процесс настройки непрерывный процесс, т.к. компания будет развиваться и документооборот будет только увеличиваться, для этого необходимо будет создавать новые политики и корректировать прежние.
4. Требуется выделение больших объемов хранения данных и их обслуживание	Для полноценных расследований инцидентов требуются данные событий, логов и т.д. за длинный промежуток времени, это может быть год, два, а, может быть, и десять лет. А если в компании работает более ста человек, то хранение и комплексная защита таких данных требует большого количества ресурсов, как финансовых, покупка жестких дисков, серверов, стоек, а также выделения для этого специального помещения, чтобы обеспечить высокую безопасность.
5. Отсутствие квалифицированных работников для работы с системой	Не каждая компания может себе позволить взять к себе в штат отдельного специалиста по информационной безопасности, что составляет определенную проблему. Почти у всех организаций в штате есть системный администратор, но возлагать на него всю ответственность по мониторингу, реагированию и расследование инцидентов нецелесообразно. У системного администратора есть свои задачи, которые он должен выполнять. Хороший специалист с высшим образованием и опытом работы нужен, т.к. он в большей части будет общаться с компанией поставщиков *DLP*-систем и настраивать все политики безопасности.
6. Существует множество способов обхода *DLP*-систем	На данный момент в интернете есть много способов обойти систему и вынести конфиденциальную информацию. Например, *DLP* защищает персональный компьютер, но любой желающий, если это не запрещает политика безопасности компании, может сфотографировать секретный документ на мониторе компьютера на свой телефон или планшет. Так же злоумышленники могут использовать стеганографию. Передача аудиосообщений тоже может с трудом обрабатываться системой, тем самым давая возможность передавать конфиденциальную информацию по аудио каналу.

Вывод по недостаткам внедрения *DLP*-систем

При существовании множества недостатков, таких как дороговизна полноценного внедрения системы организацию, наличия потенциальной возможности срабатывания этой системы против собственной компании при ее неправильном ис-

пользовании, а также при личной инициативе сотрудника обойти эту систему [2, 4]. Эти факторы подтверждают факт отсутствия идеальных систем защиты информации. Однако *DLP*-система может максимально снизить риск от непреднамеренной утечки информации, а также позволяет выявлять и предотвращать инциденты, связанные с обеспечением информационной безопасности предприятия.

Таблица 2

Преимущества внедрения DLP-системы

Преимущество	Описание
1. Учет рабочего времени сотрудников	*DLP* позволяет вести количественный и качественный учет рабочего времени сотрудников, учитывать начало и окончание рабочего дня, тем самым позволяет фиксировать, какие сотрудники опаздывают на работу, а какие остаются после рабочего дня и перерабатывают. Учитывается интенсивность их работы и активность на протяжении всего рабочего дня. Офицер безопасности может видеть развернутую картину реального положения дел в организации. Дополнением к выше перечисленному предоставляется возможность ведение записи хронометража дня, тем самым фиксируется хронология действий персонала за служебными компьютерами. Выводится информация о сайтах, на которые он заходил, какие файлы открывал, какие программы и в какой время использовал, тем самым можно точно определить, чем занимался определенный сотрудник в интересующий момент времени.
2. Оценка продуктивности сотрудников	Руководство организации часто не владеет информацией о том, что делает сотрудник в рабочее время. *DLP* позволяют настроить списки сайтов, программ по критериям: продуктивные, непродуктивные и нейтральные и далее автоматически определять, как сотрудник тратит время на работе, тем самым выявлять непродуктивных сотрудников и определять, какой объем рабочего времени был потрачен на непосредственное выполнение служебных обязанностей.
3. Незаметный режим работы	*DLP* может работать в скрытом режиме, и она будет невидима для конечного пользователя, но это может превратиться и в слежку. В интересах компании открыто информировать сотрудников о внедрении *DLP*, что позволит повысить корректность обращения сотрудников со служебной информацией, во-вторых, с большей ответственностью подходили к рабочему процессу и не доводили до расследования зафиксированных инцидентов. А если произошел инцидент, в котором виноват сотрудник, то в суде, предоставив результаты работы *DLP*, можно доказать вину подозреваемого. Скрытый режим работы *DLP* позволяет делать скриншоты экранов, даже нескольких мониторов, в режиме реального времени, а также позволяет быстро оценить, чем занимается сотрудник в данное рабочее время. Такая функция может быть активирована в определенное время, например, каждые десять минут, а также при запуске определенных программ или захода на определенные сайты, либо при вводе определенной фразы. В таком режиме осуществляется сканирование подключенных *USB, CD/DVD* устройств к компьютеру, и анализируется, какие данные передаются между ними.

Преимущество	Описание
4. Контроль обмена сообщений по электронной почте	*DLP* контролирует все основные каналы передачи информации, каждый сотрудник использует электронную почту, поэтому система поддерживает перехват сообщений почтовых служб в бесплатных почтовых сервисах, таких как *Gmail, Mail.ru* или Яндекс.Почта, а так же позволяет перехватывать сообщения по основным протоколам *POP*3, *SMTP, IMAP, MAPI.*
5. Контроль популярных мессенджеров	Иногда деловые разговоры выходят за рамки электронной почты и переходят в мессенджеры. *DLP*-системы позволяют контролировать, какие сообщение и файлы пересылаются между собеседниками в большинстве популярных мессенджеров, благодаря анализу протоколов обмена мгновенными сообщениями *MMP* (*Mail.Ru* Агент), *QIP Infium*, *PSI*), *YIM* (*Yahoo*! *Messenger*), *XMPP* (*Jabber*) (*Miranda*, *Google Talk, QIP Infium, PSI*), *OSCAR* (*ICQ/AIM*). Тем самым может перехватывать текстовые и голосовые сообщения, а также приложенные файлы, которые пересылаются в *Viber, WhatsApp, Skype* и *Telegram.*
6. Контроль сообщений в социальных сетях	Сейчас почти у каждого человека есть страничка в какой-либо социальной сети, этим любят пользоваться мошенники и с помощью социальной инженерии похищать информацию. Современная *DLP*-система позволяет в автономном режиме перехватывать все сообщения в таких социальных сетях как *Facebook*, Вконтакте, Одноклассники и другие. Кроме социальных сетей многие пользователи Интернет любят сидеть на форумах и, например, обсуждать работу. *DLP*-система позволяет контролировать общение сотрудников на форумах, онлайн-чатах, блогах и т.д.
7. Контроль облачных хранилищ	Облачные хранилища могут быть использованы сотрудником, как для резервного копирования информации, так и для ее похищения из коммерческой организации. Поэтому *DLP*-системы позволяют контролировать потоки информации, скаченные и загруженные файлы, для следующих облачных сервисов: Яндекс.Диск, *Drobox*, *OneDrive*, *Google* Диск.

Вывод по преимуществам внедрения *DLP*-систем

Достоинств внедрения *DLP*-систем в организации объективно больше. Учитывая рабочее время сотрудников, руководителю будет проще ориентироваться, кто больше сидит в социальных сетях и форумах, находясь на рабочем месте, что способствует повышению уровня трудовой дисциплины и выявляет проблемы реализации бизнес-процессов.

DLP-системы дают возможность контролировать почти все каналы информационных потоков в компании, начиная от аппаратных, позволяют анализировать информацию, не только переданную на подключенный USB-флэш накопителей, но и перенесенные в облачное хранилище Яндекс.Диск. По средствам собирания логов позволяет точно восстанавливать цепочки событий и устанавливать всех сотрудников, причастных к нарушениям.

Проектная экспертиза попытки внедрения *DLP*-системы в коммерческую организацию

При проведении апробационного эксперимента с целью детального рассмотрения возможных угроз безопасности и целостности информации, в организации сформирован «гипотетический» штат сотрудников на примере виртуального отдела по работе с персональными данными ЗСС (рис. 5). Чтобы уберечь организацию от инцидентов, следует понимать какая информация и в каком отделе может являться

конфиденциальной. Рассмотрим специфи-

Отдел информационных систем. Основными задачами этого отдела является: обеспечение штатного функционирования и эксплуатации информационно-технической инфраструктуры; организация мероприятий по повышению функционирования информационных систем; обеспечение технических мер по защите информации (ее антивирусного контроля).

кацию работы каждого из отделов.

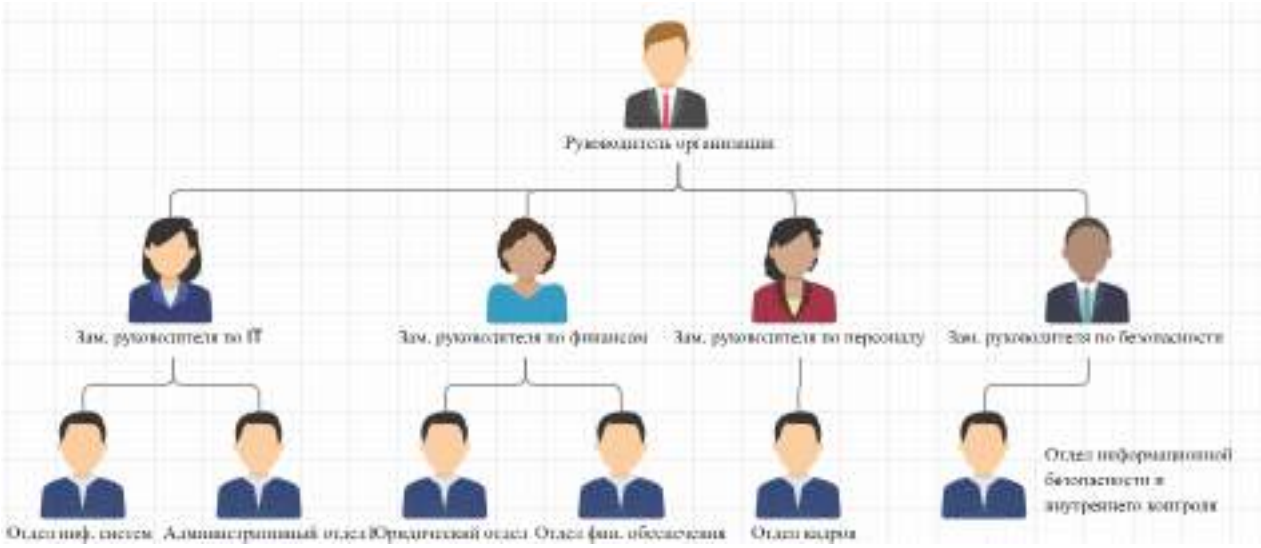

Рис. 5. Штат сотрудников ООО «ЗСС»

Административный отдел. В рамках поставленных задач отдел выполняет следующие функции: организует работу приемной у руководителя и его заместителей; организует хозяйственно-бытовое обеспечение компании; следит за выполнением поручений руководителя в установленные сроки.

Отдел финансового обеспечения. Основными задачами и функциями отдела являются: ведение бюджетного, налогового и управленческого учета; осуществление формирования полной и достоверной информации о финансовой и хозяйственной деятельности; осуществление организации ведения нормативно-справочной информации, относящейся к функциям отдела.

Отдел кадров. Занимается осуществлением формирования кадрового состава; формированием штатного расписания сотрудников; ведением табеля учета использования рабочего времени и расчета заработной платы.

Юридический отдел. Имеет следующие полномочия: проверяет на соответствие законодательству Российской Федерации и визирует проекты нормативных правовых актов компании; осуществляет правовое сопровождение деятельности компании посредством предоставления консультаций; подготавливает заключения по вопросам правового характера, возникающим в процессе деятельности компании.

Отдел информационной безопасности и внутреннего контроля. В задачи этого отдела входят: изучение кадрового состава; организация проведения служебных проверок; обеспечение в пределах своей компетенции защиты сведений, составляющих государственную тайну, и иных сведений ограниченного распространения.

Проведя анализ работы разных отделов компании, авторы пришли к выводу, что даже в небольшой организации необходимо внедрение *DLP*-системы, для обеспечения информационной безопасности и снижению рисков потери важных сведений, например, годовой отчетности, сведений о составе организации и другие [5,6].

DLP-система захватывает пакеты, передаваемые по всей сети в режиме прослушивания, и сравнивает трафик с базами сигнатур атак. Журнал отображает список атак для администратора при организации противодействия нарушителям. Данная система работает как устройство оповещения в случае атак. Работать в сети она может в двух режимах: в фоновом режиме и в режиме активного мониторинга сети.

Система имеет следующие достоинства: подключение дополнительных сенсоров для обнаружения в систему, выбор сенсоров для захвата, пауза захвата и очистка захваченных данных, отображение состояния на снимках системы. Система дополняется новыми сигнатурами с сервера. *DLP* ищет общую характеристику атак, которая заключается в том, что при их инициировании и во время выполнения атаки, процессы вторжений производят достаточный сетевой трафик (например, сканирование портов), чтобы локальные детекторы могли найти достаточные доказательства для будущей атаки и сообщить о них.

Архитектура системы предотвращения утечек информации *DLP*

Методика внедрения системы предотвращения утечек информации *DLP* в коммерческую организацию для информационной сети с использованием Больших данных [6] дополняется спроектированной архитектурой (рис. 6) с использованием специальных сетевых зондов для сбора необработанных пакетных данных. Использует эти необработанные пакетные данные для получения пакетной информации, такой как *IP*-адрес источника и адрес назначения, порты источника и назначения, флаги, длина заголовка, контрольная сумма, время жизни (*TTL*) и тип протокола.

Рис. 6. Реализация архитектуры

Сетевые зонды имеют следующий тип обязательных элементов с наличием обработки Больших данных:

1. Анализатор пакетов. Этот модуль включает в себя захват всего трафика, проходящего через сеть. Сниффер (*Sniffer*) будет установлен на конечной точке системы в сети, на которой должен быть захвачен трафик. Сниффер захватывает весь сетевой трафик, работая с сетевым адаптером в беспорядочном режиме [8].

2. Определение сигнатур атак. Сигнатуры атаки являются шаблонами атакующего трафика [9]. Сигнатуры моделируются на основе шаблона заголовка пакета, за которым следует конкретная атака. Он включает в себя подсчет пакетов от конкретной цели или конкретного источника, или порта назначения, или он может ~~даже~~ быть смоделирован с помощью других деталей в пакете, таких как размер заголовка, время жизни пакета, биты из регистра флагов, протокол.

3. Идентификация атак. Это извлечение полезной информации из захваченного локального трафика, такой как *IP*-адреса источника и назначения, тип протокола, длина заголовка, порты источника и назначения и т.д., и сравнение этих данных с моделируемыми сигнатурами атак, чтобы определить, произошла ли атака [10].

4. Сообщение о деталях атаки. Это сообщение об атаке администратору, чтобы он мог предпринять необходимые действия. Отчетность включает в себя указание деталей атаки, таких как *IP*-адреса источника и жертвы, временная метка атаки и, что более важно, тип атаки [10, 11].

Заключение

При правильно настроенной DLP-системе, которая будет контролировать все возможные каналы передачи информации, а не только часть из них, предотвращается 100% случайных утечек и некоторая часть умышленных. Практика показывает, что эффективность систем, развернутых в коммерческих организациях, измеряется не только количеством отловленных утечек, но и деньгами. Если организацию устраивает то, как хранится и обрабатывается конфиденциальная информация, значит система работает эффективно. Эффективность собственно программного обеспечения зависит от того, как им пользоваться – можно неэффективно пользоваться хорошей системой, а можно эффективно – плохой. Здесь необходимо учитывать, насколько точно категорированы данные в организации, как категории присваиваются новым и входящим документам, как формализованы критерии легитимности передачи конфиденциальных данных, как эффективно действует система поощрений и наказаний за соблюдение правил обращения с конфиденциальной информацией и т.д. Часто сам факт наличия в компании системы защиты от утечек информации, ставший достоянием гласности, уже эффективен. Большинство сотрудников будет внимательнее относиться к передаче конфиденциальных данных.

Проектирование *DLP*-системы с методикой, основанной на сигнатурах и использовании Больших данных, имеет существенные улучшения в ряде причин [6, 7, 8]. Система сможет успешно захватывать пакеты, передаваемые по всей сети в режиме прослушивания, и сравнивает трафик с базами сигнатур нарушений. Журнал нарушений отображает список атак для администратора для противодействия нарушителям.

СПИСОК ЛИТЕРАТУРЫ

1. Карев А.С., Бирих Э.В., Сахаров Д.В., Виткова Л.А. Проблемы информационной безопасности в интернете вещей // В сборнике: Интернет вещей и 5G 2016. С. 66-70.
2. Пат. 2472211Российская федерация. Способ защиты информационно-вычислительных сетей от компьютерных атак / Андрианов В.И., Бухарин В.В., Кирьянов А.В., Липатников В.А., Санин И.Ю., Сахаров Д.В., Стародубцев Ю.И. № 2011147613/08; заявл. 23.11.2011; опубл. 10.01.2013.
3. Костарев С.В., Липатников В.А., Сахаров Д.В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 120-125.
4. Виткова Л.А., Проноза А.А., Сахаров Д.В., Чечулин А.А. Проблемы безопасности информационной сферы в условиях информационного противоборства // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018): сб. науч. ст. VII Международ. науч.-техн. и науч.-метод. конф. / под ред. С.В. Бачевского. 2018. С. 191-195.
5. Дубровин Н.Д., Ушаков И.А., Чечулин А.А. Применение технологии больших данных в системах управления информацией и событиями безопасности / Актуальные проблемы инфотелекоммуникаций в науке и образовании: сб. науч. статей V Международ. науч.-техн. и науч.-метод. конф. 2016. С. 348-353.
6. Котенко И.В., Ушаков И.А. Технологии больших данных для мониторинга компьютерной безопасности // Защита информации. Инсайд. 2017. № 3 (75). С. 23-33.
7. Василишин Н.С., Ушаков И.А., Котенко И.В. Исследование алгоритмов анализа сетевого трафика с использованием технологий больших данных для обнаружения компьютерных атак // Информационные технологии в управлении (ИТУ-2016): материалы 9-й конф. по проблемам управления. 2016. С. 670-675.
8. Дешевых Е.А., Ушаков И.А., Котенко И.В. Обзор средств и платформ обработки больших данных для задач мониторинга информационной безопасности // Информационная безопас-

ность регионов России (ИБРР-2015): материалы конф. 2015. С. 67.
9. Ушаков И.А., Котенко И.В. Модель обнаружения внутренних нарушителей на основе использования технологий больших данных // Региональная информатика и информационная безопасность 2017. С. 253-254.
10. Котенко И.В., Пелёвин Д.В., Ушаков И.А. Общая методика обнаружения инсайдера компьютерной сети на основе технологий больших данных //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2019): сб. науч. статей VIII Международ. науч.-техн. и науч.-метод. конф. / под. ред. С.В. Бачевского. 2019. С. 572-576.
11. Косов Н.А., Гельфанд А.М., Лаптев А.А. Анализ темных данных для обеспечения устойчивости информационных систем от нарушения конфиденциальности или несанкционированных действий // Colloquium-Journal. 2019. №13-2 (37). С. 100-103.

1. Karev A.S., Birikh E.V., Sakharov D.V., Vitkova L.A. Problems of information safety in thing Internet // *In Proceedings: Thing Internet and 5G 2016*. pp. 66-70.
2. Pat. 2472211 the Russian Federation. *Method for Information-Computer Network Protection against Computer Intrusions* / Andrianov V.I., Bukharin V.V., Kiriyanov A.V., Lipatnikov V.A., Sanin I.Yu., Sakharov D.V., Starodubtsev Yu.I. No.2011147613/08; applied: 23.11.2011.; published: 10.01.2013.
3. Kostarev S.V., Lipatnikov V.A., Sakharov D.V. Model of audit and control results transfer in automated system of company management of integrated structure // *Problems of Information Safety. Computer Systems*. 2015. No.2. pp. 120-125.
4. Vitkova L.A., Pronoza L.A., Sakharov D.V., Chechulin A.A. Safety problems of information sphere under conditions of information confrontation // *Urgent Problems of Info-telecommunications in Science and Education (APINO 2018): Proceedings of the VII-th Inter. Scientif.-Tech. and Science-Method. Conf.* / under the editorship of S.V. Bachevsky. 2018. pp. 191-195.
5. Dubrovin N.D., Ushakov I.A., Chechulin A.A. Application of large database in control systems of information and safety events / *Urgent Problems of Info-telecommunications in Science and Education: Proceedings of the V-th Inter. Scientif.-Tech. And Scientif.-Method. Conf. 2*016. pp. 348-353.
6. Kotenko I.V., Ushakov I.A. Large database technologies for computer safety monitoring // *Information Protection. Inside*. 2017. No.3. pp. 23-33.
7. Vasilishin N.S., Ushakov I.A., Kotenko I.V. Analysis algorithm investigations of network traffic using large database technologies for computer intrusion detection // *Information Technologies in Management (ITU-2016): Proceedings of the IX-th Conf. on Management Problems*. 2016. pp. 670-675.
8. Deshovykh E.A., Ushakov I.A., Kotenko I.V. Review of means and platforms of large database processing // *Information Safety of Russian Regions (IBRR-2015): Proceedings of the Conf. 2015.* pp. 67.
9. Ushakov I.A., Kotenko I.V. Model of inner disturber detection based on large database technology use // *Regional Informatics and Information Safety 2017*. pp. 253-254.
10. Kotenko I.V., Pelyovin D.V., Ushakov I.A. General procedure for detection of computer network insider based on large database technologies // *Urgent Problems of Info-telecommunications in Science and Education (APINO 2019): Proceedings of the VIII-th Inter. Scientif.-Tech. and Scientif.-Method. Conf.* / under the editorship of S.V. Bachevsky. 2019. pp. 572-576.
11. Kosov N.A., Gelfand A.M., Laptev A.A. Dark data analysis to ensure information system stability from confidentiality breaches or non-authorized actions // *Colloquium-Journal. 2019*. No.13-2 (37). pp. 100-103.

Ссылка для цитирования:
Андрианов В.И., Сивков Д.И., Юркин Д.В. Методика внедрения системы предотвращения утечек информации DLP в коммерческую организацию для информационной сети с использованием больших данных // Вестник Брянского государственного технического университета. 2020. № 6. С. 38-48. DOI: 10.30987/1999-8775-2020-6-38-49.

Статья поступила в редакцию 10.02.20.
Рецензент: к.т.н., доцент Брянского государственного технического университета Рытов М.Ю., член редсовета журнала «Вестник БГТУ».
Статья принята к публикации 25.05.20.

Сведения об авторах:

Андрианов Владимир Игоревич, к.т.н., доцент кафедры «Защищенные системы связи», Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, e-mail: vladimir.i.andrianov@gmail.com.

Сивков Дмитрий Игоревич, бакалавр кафедры «Защищенные системы связи», Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, e-mail: 485280@mail.ru.

Юркин Дмитрий Валерьевич, к.т.н., доцент кафедры «Защищенные системы связи», Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, e-mail: dvyurkin@ya.ru.

Andrianov Vladimir Igorevich, Can. Sc. Tech., Assistant Prof. of the Dep. "Protected Communication Systems", Bonch-Bruevich State Telecommunication University of Saint-Petersburg, e- mail: vladimir.i.andrianov@gmail.com.
Sivkov Dmitry Igorevich, Bachelor of the Dep. "Protected Communication Systems", Bonch-Bruevich State Telecommunication University of Saint-Petersburg, e-mail: 485280@mail.ru.
Yurkin Dmitry Valerievich, Can. Sc. Tech., Assistant Prof. of the Dep. "Protected Communication Systems", Bonch-Bruevich State Telecommunication University of Saint-Petersburg, e- mail: dvyurkin@ya.ru.