УДК 004.056.53
DOI 10.34822/1999-7604-2020-1-35-42

ПОСТРОЕНИЕ ВИРТУАЛЬНОЙ МОДЕЛИ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИИ С ИСПОЛЬЗОВАНИЕМ СИСТЕМЫ INFOWATCH TRAFFIC MONITOR

А. М. Шабалин ✉, Е. А. Калиберда
Омский государственный технический университет, Омск, Россия
✉*E-mail: sham.omsk@gmail.com*

В статье анализируется специфика процесса защиты корпоративной сети от внутренних и внешних угроз информационной безопасности. Особую опасность, по мнению авторов, представляют собой всевозможные виды утечек корпоративной информации и персональных данных, возникающие вследствие действий так называемых «внутренних злоумышленников», или инсайдеров, против которых наиболее эффективным средством защиты является класс программного обеспечения Data Loss Prevention (DLP-системы). InfoWatch Traffic Monitor 6.11 – российский программный продукт, сертифицированный в системе Федеральной службы по техническому и экспортному контролю России и являющийся одним из мировых лидеров в данном классе программного обеспечения. На основании полученной лицензии от компании InfoWatch в виртуальной лаборатории Омского государственного технического университета был создан специализированный стенд, позволяющий произвести настройку и проверку данной DLP-системы, определить политику безопасности, обеспечить контроль информационных потоков в компании, а также проанализировать выявленные инциденты. Для этого была разработана виртуальная модель внедрения DLP-системы в комплексную систему защиты информации организации, в которой были определены объекты информационной безопасности и разработаны соотвествующие политики для предотвращения утечки данных и выявления возможных инцидентов, осуществлены перехваты конфиденциальной информации по контролируемым каналам связи.

Ключевые слова: внутренние угрозы, модель защиты информации, DLP-система, InfoWatch, виртуальный стенд.

BUILDING A VIRTUAL MODEL FOR CORPORATE INFORMATION PROTECTION USING INFOWATCH TRAFFIC MONITOR SYSTEM

A. M. Shabalin ✉, E. A. Kaliberda
Omsk State Technical University, Omsk, Russia
✉*E-mail: sham.omsk@gmail.com*

The article analyzes the features of the process for protecting the corporate network from internal and external threats to information security. According to the authors, a particular danger are all kinds of corporate information and personal data leaks arising from the actions of so-called “internal intruders” or insiders, against which the Data Loss Prevention software (DLP systems) is the most effective measure. InfoWatch Traffic Monitor 6.11 is a Russian software product certified by the Federal Service for Technical and Export Control and considered to be one of the world leaders in a given class of software. Based on the license obtained from InfoWatch, in the virtual laboratory of Omsk State Technical University, a specialized stand is created, allowing to configure and verify the DLP system, determine security policies, ensure control of information flows in the company and analyze incidents that have been identified. For these purposes a virtual model for introducing a DLP system into a comprehensive information protection system is developed, where information security objects are identified and appropriate policies are established to prevent data leakage and

the identification of possible incidents, and confidential information is intercepted via controlled communication channels.

Keywords: internal threats, model for information protection, DLP system, InfoWatch, virtual stand.

Современный анализ угроз информационной безопасности (далее – ИБ) начинается с их классификации и выявления из них самых актуальных. На настоящий момент теория защиты информации включает в себя несколько классификаций, среди которых наиболее популярной является классификация по источникам информационных угроз с делением их на *внешние и внутренние* [1].

Еще в недалеком прошлом внешний злоумышленник (хакер) рассматривался как основная угроза, и в течение многих лет компании боролись с несанкционированным доступом, а защита от вторжения извне достигла ощутимых результатов. Сейчас пробивать внешнюю защиту компании становится все труднее, а значит, можно получить необходимую информацию от сотрудника компании, успешно прошедшего аутентификацию и получившего доступ к корпоративной информации. Поэтому на сегодняшний день ситуация изменилась корренным образом, внутренние злоумышленники (инсайдеры), действующие в соответствии с личными мотивами, становятся не менее, а порой и более актуальной угрозой ИБ компании, и с каждым годом ситуация усугубляется [2].

Так, за первое полугодие 2019 года компания InfoWatch зафиксировала 1 276 случаев утечки информации из компаний, что на 22 % больше, чем за аналогичный период 2018 года (695 случаев по вине внутренних нарушителей) [3].

Системы выявления и предотвращения утечек (Data Loss Prevention, DLP-системы) появились примерно в 2006 году. Их принцип работы заключается в анализе внутреннего трафика, который существует в защищаемой сети предприятия. Качественно подобранная и внедренная DLP-система способна защитить от халатности и ошибочных действий сотрудников и предотвратить практически все возможные сценарии утечки информации посредством внутренних каналов [4, 5].

В декабре 2019 года российская компания InfoWatch представила очередную версию своей DLP-системы InfoWatch Traffic Monitor 6.11. Омский государственный технический университет получил лицензию на три основных продукта компании (опционально могут быть подключены дополнительные компоненты):

- InfoWatch Traffic Monitor (IWTM) – главный компонент, предназначенный для анализа трафика компьютерной сети компании;
- InfoWatch Device Monitor Monitor (IWDM) – компонент для защиты рабочих станций, имеющий серверную и клиентскую часть;
- InfoWatch Crawler – компонент для контроля конфиденциальной информации на сетевых хранилищах данных.

Для работы с данными программными продуктами в Омском государственном техническом университете была организована специализированная лаборатория, где с помощью современных средств виртуализации были произведены настройка и проверка программного обеспечения, определены политики безопасности, обеспечен контроль информационных потоков в компании, а также проанализированы выявленные инциденты. В лаборатории для каждого рабочего места был разработан виртуальный стенд. Принцип работы стендов представлен на рис. 1.

В качестве аппаратной платформы был выбран один из двух серверов лаборатории Dell PowerEdge R530 (2U/ 2xE5-2650v4 (2.2GHz/12Core/30Mb)/ 6x16Gb RDIMM(2400) / 8x4Tb SATA 7,2k/ DVDRW/ 4xGE/ 2x750W).

На данном сервере был организован дисковый массив RAID-5 и установлен гипервизор VMWare ESXi Server 6.5, который позволяет создавать гибкую виртуальную инфраструктуру в соответствии с потребностями любых организаций.

Каждый стенд может быть упрощенно представлен в виде логической топологии, изображенной на рис. 2, и организуется на базе стандартного персонального компьютера с менеджером виртуальных машин VMware vSphere Client для установки соединения по локальной сети аудитории с VMWare ESXi Server.

Внутри гипервизора создается инфраструктура из трех виртуальных машин, на которых разворачивается программный комплекс InfoWatch Traffic Motnitor, состоящий из двух серверов IWTM и IWDM, а также клиентского компьютера, с которого эмулируются действия инсайдера.

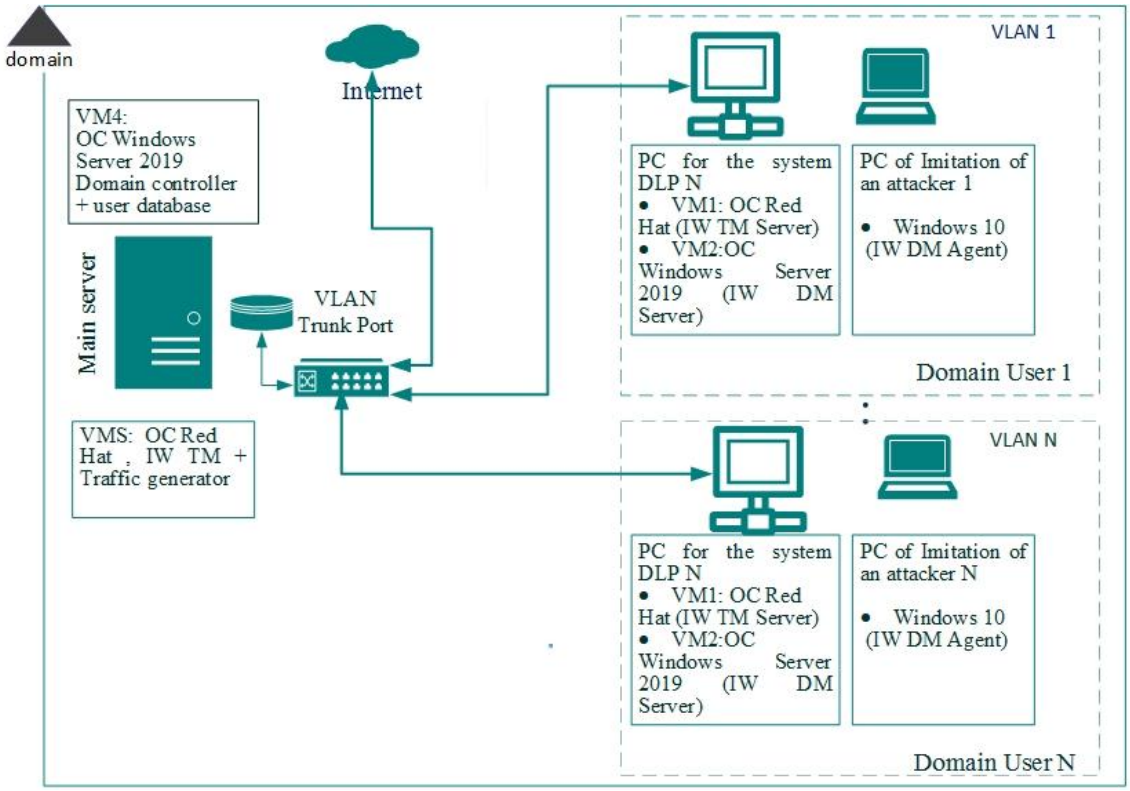

Рис. 1. Схема работы лаборатории InfoWatch
Примечание: составлено авторами.

Все три компьютера находятся в одной виртуальной локальной сети (VLAN) и соединяются с помощью виртуального коммутатора VMWare Switch, а также имеют доступ к сети Интернет через маршрутизатор Mikrotik Cloud Hosted Router (CHR), который специально предназначен для работы в виртуальных средах для 64-битных платформ и может быть использован с большинством популярных гипервизоров, таких как VMWare, Hyper-V, VirtualBox, KVM и другие.

В результате на созданном виртуальном стенде поэтапно были проведены следующие подготовительные работы [6]:

1. Установлены и сконфигурированы:

- операционная система Red Hat Linux, СУБД Postgres, сервер IWTM;
- операционная система MS Windows 2019 Server, СУБД Postgres, сервер IWDM и модуль InfoWatch Crawler;
- служба каталогов Active Directoty и служба доменных имен DNS;
- клиентская операционная система MS Windows 10, под управлением которой компьютер введен в созданный домен, с сервера была централизованно установлена агентская часть IWDM.

2. Проведена интеграция программных продуктов InfoWatch со службой Active Directory.

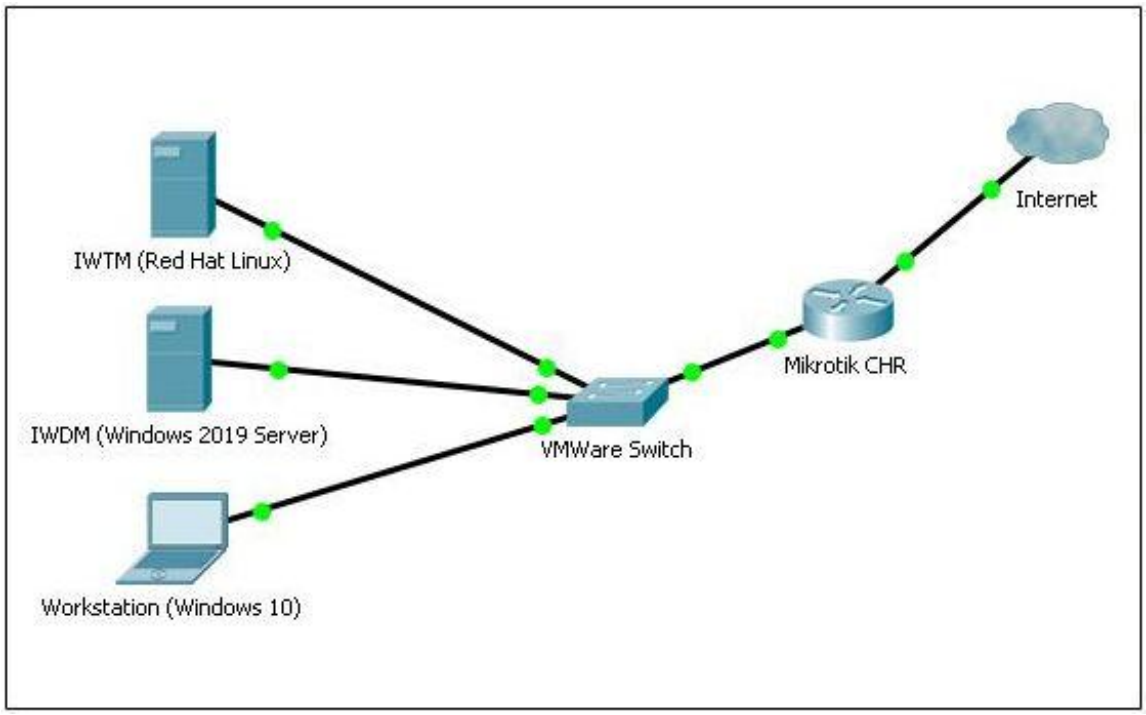

Рис. 2. Логическая топология разработанной виртуальной сети
Примечание: составлено авторами.

Процедура внедрения DLP-системы в комплексную систему защиты информации организации должна проходить строго поэтапно. Алгоритм действий, который разработан авторами статьи, позволяет упорядочить все действия, упростить задачу по внедрению DLP-системы, содержит 4 последовательных этапа (рис. 3, 4) [7].

Для *первого этапа* предпроектного исследования характерны следующие процессы:

1. Проведение аудита защищенности информации и оценки рисков.
2. Составление перечня конфиденциальной информации и схемы разграничения прав доступа к данным.
3. Создание нормативно-правового поля при внедрении DLP.
4. Расчет экономической эффективности внедрения.
5. Выбор подходящей DLP-системы и ее комплектации в соответствии с потребностями и ресурсами компании.

На *втором этапе* установки DLP-системы осуществляются инсталляции и первичная настройка системы, а также создание политики безопасности, основанной на потребностях и деятельности организации.

На *третьем этапе* опытной эксплуатации DLP-системы необходимо провести следующие работы:

1. Анализ защищаемых сетевых каналов и согласование набора технических документов, описывающих окончательное проектное решение.
2. Инвентаризация носителей и маршрутов движения данных, которым угрожают несанкционированные действия и на которые будет устанавливаться DLP-система.
3. Тестирование работоспособности системы в реальных условиях.

Четвертый этап процесса ввода в промышленную эксплуатацию имеет следующие составляющие:

1. Обучение специалистов, ответственных за работу с DLP-системой.
2. Осуществление анализа опытного запуска DLP-системы (при необходимости проведение дополнительной настройки системы с минимизацией ложных срабатываний).
3. Запуск системы в промышленную эксплуатацию.

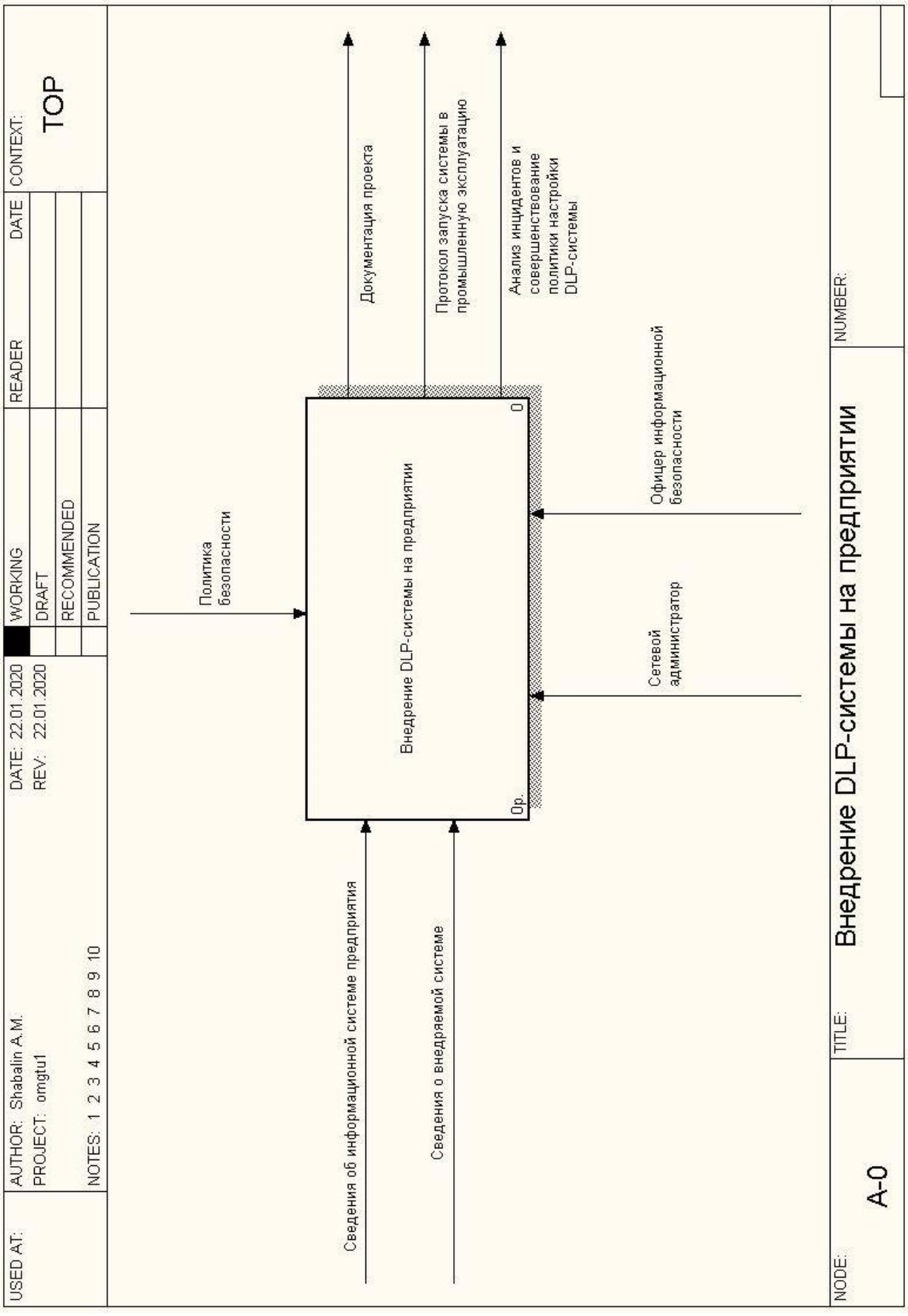

Рис. 3. Характеристика процесса внедрения DLP-системы на предприятии
Примечание: составлено авторами.

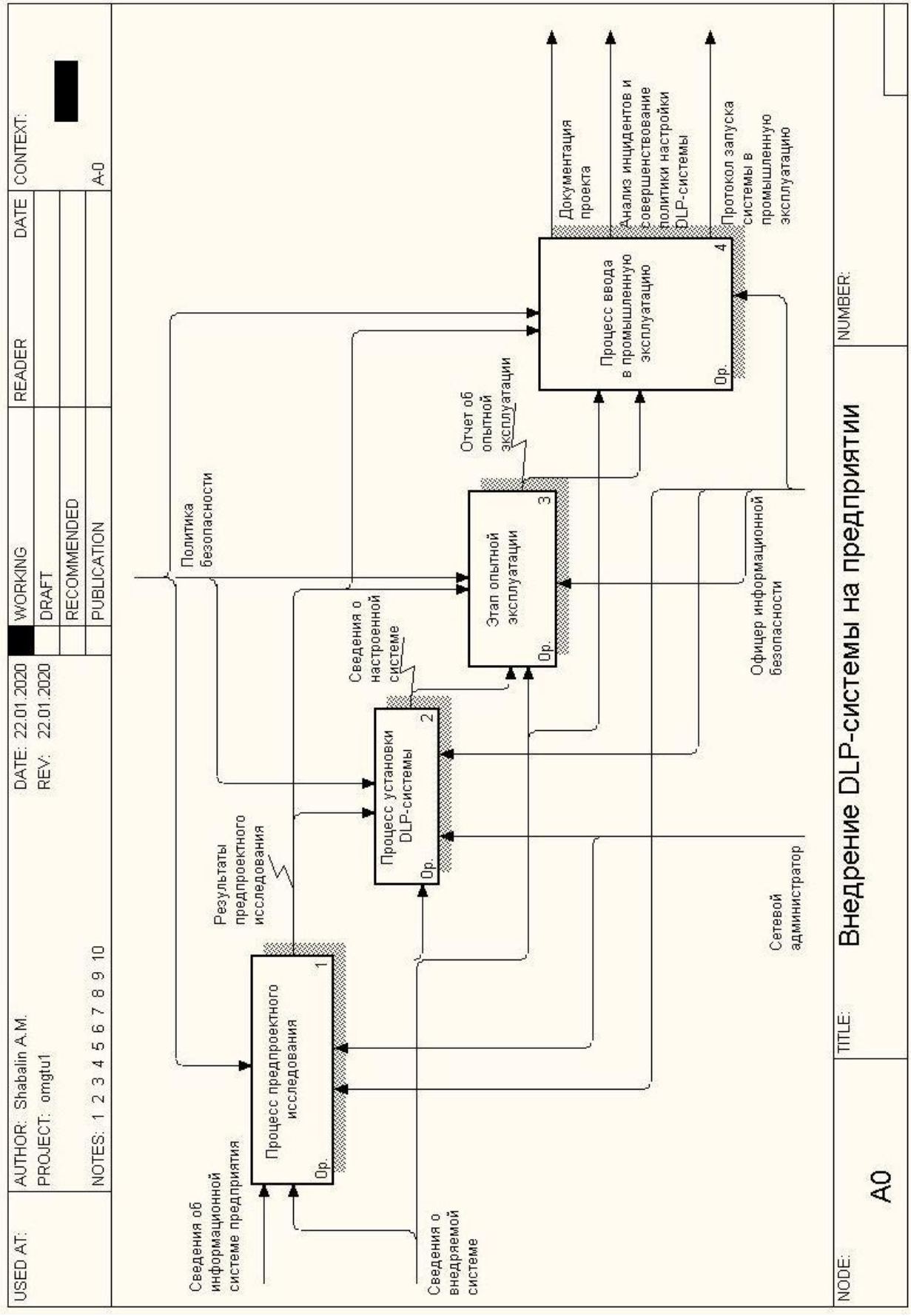

Рис. 4. Декомпозиция процесса внедрения DLP-системы на предприятии
Примечание: составлено авторами.

В результате выполнения всех перечисленных действий можно получить качественно функционирующую DLP-систему. При этом важно помнить, что настройка системы – это процесс, не прекращающийся на протяжении всего периода эксплуатации продукта.

На созданном виртуальном стенде были разработаны и апробированы следующие политики безопасности для виртуальной организации:

- политика перехвата эталонных документов;
- политика перехвата своей категории и термина;
- политика перехвата текстового объекта с использованием регулярных выражений;
- политика перехвата документа с эталонной печатью;
- работа «белого» списка устройств на клиентских компьютерах;
- работа «черного» списка приложений на клиентских компьютерах.

В результате применения указанных политик были проведены перехваты конфиденциальной информации; пользователю на клиентском компьютере был определен список внешних устройств, с которыми ему можно работать, и отключено не разрешенное для использования в рабочее время программное обеспечение.

Помимо этого, по различным каналам были осуществлены перехваты конфиденциальной информации, отправленной пользователем в виде:

- электронного письма по протоколам SMTP (почтовый клиент Mozilla ThunderBird) и HTTP (web-почта);
- снимков экранов и автоматического распознавания их с помощью OCR Tesseract (подключение дополнительного программного обеспечения);
- текстовых сообщений – в программах Skype и Pidgin (по протоколу XMPP);
- событий печати – на локальном принтере;
- данных, скопированных в буфер обмена;
- данных, копируемых на внешнее устройство (USB Flash).

Кроме того, было произведено обнаружение конфиденциальной информации в папке пользователя с помощью программы InfoWatch Crawler.

На завершающем этапе работы использовался аналитический функционал системы InfoWatch Traffic Monitor для создания отчетов о выявленных инцидентах и анализа полученных данных:

1. Организованы выборки событий по созданным условиям.
2. Сгенерированы отчеты по созданным условиям на основе собранных на стенде данных.

Итак, в результате построения и внедрения виртуальной модели был успешно апробирован функционал по обеспечению защиты конфиденциальных данных организации от утечек, вызванных неправомерными действиями сотрудников (инсайдеров), совершенными как целенаправленно, так и вследствие проявленной халатности или невнимательности. На основе гипервизора VMWare ESXi Server 6.5 была развернута виртуальная лаборатория, на которой апробировался функционал DLP-системы InfoWatch Traffic Monitor 6.11. Работа по корпоративной защите от внутренних угроз включала сборку, установку, тестирование, использование и обслуживание специализированных программно-аппаратных комплексов по перехвату и анализу трафика данных, циркулирующего в организации. В DLP-системе созданы объекты безопасности, разработаны политики безопасности, состоящие из соответствующих наборов правил. Политики ИБ применены на практике для перекрытия возможных каналов утечки данных и выявления инцидентов безопасности, для чего в перехваченном трафике использовались механизмы фильтрации.

Таким образом, построение модели защиты корпоративной информации в виртуальной лаборатории является, на наш взгляд, обязательной составляющей процесса внедрения DLP-системы в систему обеспечения информационной безопасности компании, так как только продуманная поэтапная работа на основе виртуальной модели, созданной с учетом конкретных потребностей предприятия, позволяет применять новые виды политики безопасности и проверять их работоспособность перед применением в реальной компьютерной сети компании.

Литература

1. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. СПб. : Питер, 2008. 320 с.

2. Шабалин А. М. Основные подходы к типологии внутренних нарушителей корпоративной информационной безопасности // Современная наука: проблемы и перспективы развития : материалы III Международ. науч.-практ. конф. : сб. ст. : в 3 ч. Омск : ОмГА, 2019. Ч. 3. С. 27–31.

3. Глобальное исследование утечек конфиденциальной информации в первом полугодии 2019 года. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/Global_Data_Leaks_Report_2019_half_year.pdf?rel=1 (дата обращения: 20.01.2020).

4. Угрозы информационной безопасности: обзор и оценка. Комплексная защита информации на предприятии. URL: http://rus.safensoft.com/security.phtml?c=791 (дата обращения: 20.01.2020).

5. Пелешенко В. С., Мирошников Д. А., Емельянов Е. А. Анализ современных DLP-систем защиты конфиденциальных данных от внутренних угроз // Новые информационные технологии и системы. 2015. № 11. С. 176–179.

6. InfoWatch Traffic Monitor. Руководство пользователя. М. : АО «Инфовотч», 2017. 522 с.

7. Шабалин А. М. Особенности внедрения DLP-систем в бизнесс-процессы современных компаний // Наука и общество: проблемы современных исследований : материалы XIII Международ. науч.-практ. конф. : сб. ст. : в 3 ч. Омск : ОмГА, 2019. Ч. 1. С. 107–111.