Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

Важной отличительной особенностью информационного пространства, которая позволяет рассматривать его именно с такой точки зрения, является то, что в отличие от других пространств, где физическую географию определяет власть, в информационном пространстве задают структуру власти информация и знания.

Значимость в информационном пространстве для информационной политики имеют те его компоненты и процессы, воздействие на которые средствами и методами информационной политики позволяет влиять на перспективы, на конкретные лица, которые принимают решения, контролировать системы сбора, обработки, хранения и передачи информации, преумножать ресурсы

Государственная информационная политика по обеспечению информационной безопасности Союзного государства в условиях информационно-психологической войны является составной частью государственной политики по обеспечению национальной безопасности в части, касающейся деятельности системы органов государственной власти по достижению национальных интересов страны и обеспечению информационно-психологической безопасности личности, общества и государства в условиях непосредственной угрозы развязывания государствами-участниками информационного противоборства крупномасштабной информационно-психологической агрессии (информационно-психологической войны) в отношении Союзного государства.

Список литературы

1. В.Е. Политические и социальные аспекты информационной безопасности: монография. – Таганрог: издатель С.А. Ступин, 2015. – 352

2. Брусницин Н.А.Информационная война и безопасность – М.: Вита-Пресс, 2001. – 280 с.

3. Манойло А.В. Государственная информационная политика в особых условиях: монография. М.: МИФИ, 2003. – 218 с.

4. Панарин И.Н. Информационная война и коммуникации. – М.: Горячая линия – Телеком, 2014. – 236 с.

5. Хорев А.А. Техническая защита информации: учеб. пособие для студентов вузов. В 3-х т. Т. 1. Технические каналы утечки информации. – М.: НПЦ «Аналитика», 2008. – 436 с.

ОЦЕНКА ЭФФЕКТИВНОСТИ РАБОТЫ DLP-СИСТЕМЫ ПО ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

В.В. МАЛИКОВ, М.А. БАБИЧ, А.В. МАКАТЕРЧИК

Белорусский государственный университет информатики и радиоэлектроники

В настоящее время, как правило, главными экономическими активами компаний и государств являются объекты интеллектуальной собственности, полученные в результате интеллектуальной деятельности с затратой значительных материальных и финансовых ресурсов. Несанкционированный доступ к таким активам приводит к их краже, что негативно влияет на экономику стран и приводит к банкротству компаний.

Обеспечение защиты от утечки конфиденциальной информации является сложной и многоуровневой задачей, которая включает в себя разграничение уровней досту-

па у сотрудников, составление документов о неразглашении, постоянное обучение сотрудников, внедрение технических средств и систем защиты информации.

Внедрение и использование DLP-систем позволяет эффективно автоматизировать ряд задач по защите конфиденциальной информации от утечки по технических каналам. Под DLP-системой (Data Loss Prevention) будем понимать программно-аппаратный комплекс, предназначенный для предотвращения утечек конфиденциальной информации за пределы корпоративной системы / сети на основе анализа потоков данных, входящих / выходящих за пределы такой системы / сети.

Современная DLP-система, как правило, состоит из нескольких модулей, функционирующих на выделенных серверах, на рабочих местах сотрудников компании (персональных компьютерах, рабочих станциях и т.д.), а также на специализированных рабочих станциях службы безопасности.

Для оценки эффективности была выбрана DLP-система «SecureTower» российской компании Falcongaze [1], которая представляет собой программный продукт, позволяющий решать задачи по защите конфиденциальной информации от утечки по технических каналам.

В рамках исследования эффективности проведено:

1. Тестирование программной среды функционирования DLP-системы на предмет поддерживаемых операционных систем (ОС) (таблица 1). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro» [2]).

2. Тестирование эффективности перехвата данных DLP-системой в приложениях, использующих протоколы: POP3, SMTP, HTTP и др. (таблица 2). Назначение портов приложений использовались по умолчанию. Эффективность перехвата оценивалась в % от детекции сформированных тестовых баз из 20 файлов / сообщений в 2-х режимах DLP-системы (настройки по умолчанию / специальная настройка параметров). Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro»).

3. Тестирование эффективности DLP-системы на стеганографические технологии модификации файлов (таблица 3). В качестве эксперимента 2 тестовых файла (формат: doc, rar; объем: до 50 КБ) с конфиденциальной информацией с использованием стенографического ПО «OpenPuff» **(**v.4.00 /настройки качества: по умолчанию/, LSB-метод) [3] встраивались в файл-контейнер (формат: png, jpg, pdf). Эффективность перехвата оценивалась в % от детекции сформированной тестовой базы из 6 файлов. Моделирование проводилось на физических и виртуальных вычислительных машинах (ПО «VMware Workstation Pro»).

Таблица 1 – Тестирование программной среды функционирования DLP-системы

Параметр сравнения	Поддерживаемые ОС		
Наименование структурного компонента для инсталляции DLP-системы	Серверное оборудование	Клиентская часть (работа с консолью)	Конечные точки (для агентской схемы)
Наименование ОС	Microsoft Windows Server 2008/2012/2016 (x64)	Microsoft Windows Vista/7/8/10/2008/2012/2016 (x86/x64)	Microsoft Windows XP SP3/Vista/7/8/10/Server 2003/2008/2012/2016 (x86/x64)
Результат тестирования	Соответствует заявленным	Соответствует заявленным	Соответствует заявленным

Таблица 2 – Тестирование эффективности перехвата данных DLP-системой

Протокол	Порт (по молчанию)	Результат тестирования перехвата данных		
		Поддержка протокола	Эффективность перехвата, % /файл, сообщение/	
			настройки по умолчанию	с настройкой параметров
POP3	110	да	90	95
SMTP	25	да	95	100
IMAP	143, 993	да	90	95
OSCAR	5190	да	90	95
HTTP	80, 8080	да	95	100
FTP	20, 21	да	90	95
XMPP	5222	да	95	100
Mail.Ru Агент	2041, 2042, 443	да	95	100
Yahoo	23,80	да	95	100
MAPI	1024-65535	да	90	100

Таблица 3 – Тестирование эффективности DLP-системы на стеганографические технологии модификации

Модификация исходного файла / метод	Наименование технологии детектирования DLP-системы	
	«Цифровой отпечаток» (Digital Fingerprints)	Контрольная сумма (хэш)
	Эффективность перехвата (файл), %	
да /стеганография (LSB)	0	0

На основании проведенного исследования эффективности работы DLP-системы по защите конфиденциальной информации от утечки по технических каналам можно сделать следующие выводы:

1. Программная среда функционирования DLP-системы Falcongaze «SecureTower» в настоящее время поддерживает все основные ОС семейства Microsoft «Windows» (таблица 1).

2. Внедрение и использование DLP-системы позволяет эффективно автоматизировать задачи по защите конфиденциальной информации от утечки по технических каналам. Эффективность перехвата данных DLP-системой по заданному перечню протоколов / портов составила от 90 % до 100 % (таблица 2).

3. Использование DLP-системы в настоящее время не позволяет детектировать стеганографические технологии модификации файлов.

Список литературы

1. Falcongaze «SecureTower» // falcongaze.ru [Электрон. ресурс]. – 2010-2017. – Режим доступа: https://falcongaze.ru/. – Дата доступа: 22.04.2017.

2. VMware Workstation Pro // vmware.com [Электрон. ресурс]. – 2017. – Режим доступа: http://www.vmware.com/ru/products/workstation.html. – Дата доступа: 22.04.2017.

3. OpenPuff team // download.cnet.com [Электрон. ресурс]. – 2017. – Режим доступа: http://download.cnet.com/windows/openpuff-team/3260-20_4-10146585-1.html. – Дата доступа: 23.04.2017.