Н. П. Лаврентьев, А. В. Мамаев

АНАЛИЗ СИСТЕМ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ОТ УТЕЧЕК С ЦЕЛЬЮ ЗАКРЫТИЯ ВОЗМОЖНЫХ УЯЗВИМОСТЕЙ

В настоящее время наиболее актуальной становится внутренняя безопасность организаций. Если раньше основным направлением защиты корпоративных сетей являлась защита от внешних угроз и попыток взлома систем снаружи, то сейчас в мире 80 % утечек происходят из-за слабой внутренней защиты [1]. Средства контроля доступа и предотвращения утечки информации направлены, главным образом, на защиту от несанкционированного доступа и несанкционированного копирования информации и малоэффективны для защиты от внутренних нарушителей, имеющих к этой информации легальный доступ. В связи с этим в настоящее время особенно активно развивается рынок специализированных систем обнаружения и предотвращения утечек информации (Information Leakage Detection and Prevention, или сокращенно ILDP) [2]. Наибольшего эффекта позволяют добиться комбинированные ILDP системы, сочетающие в себе возможности как сетевых, так и хостовых систем. В ходе работы рассматривались следующие ILDP системы:

- PortAuthority 5.0;
- Digital Guardian;
- Vontu 7.0;
- Reconnex;
- McAfee Data Loss Prevention Host;
- InfoWatch Enterprise Solution.

Данные системы представляют собой специализированные программные комплексы, предназначенные для выявления несанкционированных действий пользователей, связанных, в частности, с попыткой передачи конфиденциальной информации за пределы контролируемой зоны [3]. Основными компонентами являются:

- модули-датчики, устанавливаемые на рабочие станции пользователей и обеспечивающие сбор информации о событиях, регистрируемых на этих станциях;
- модуль анализа данных, собранных датчиками, с целью выявления несанкционированных действий пользователей, связанных с утечкой конфиденциальной информации;
- модуль реагирования на выявленные несанкционированные действия пользователей;
- модуль хранения результатов работы системы;
- модуль централизованного управления компонентами системы мониторинга.

Датчики систем мониторинга устанавливаются на те рабочие станции, на которых пользователи работают с конфиденциальной информацией. На основе настроек, заданных администратором безопасности, датчики системы позволяют контролировать доступ приложений пользователей к конфиденциальной информации, а также накладывать ограничения на те действия, которые пользователь может выполнить с этой информацией [4].

Проведенный анализ показал, что наибольшая эффективность защиты достигается при комплексном подходе к решению проблемы. Работа системы безопасности будет неэффективна, если не будет своевременного оповещения внутренней службы безопасности о попытках нарушения политик информационной безопасности. Применяющиеся для этого механизмы дистанционного мониторинга и управления в существующих системах защиты информации используют в качестве канала связи имеющуюся локальную вычислительную сеть. И это их слабое место! Внутренний нарушитель имеет возможность воздействия на данную сеть и может обеспечить для совершения противоправных действий достаточный временной интервал, когда контроль за информационными

ресурсами не будет осуществляться, а значит, говорить о высокой степени защиты информации не представляется возможным. Чтобы улучшить механизм защиты, рассмотрим нарушителя подробнее.

Обобщенная модель нарушителя для анализируемых средств защиты информации предполагает, что в качестве потенциальных злоумышленников выступают сотрудники компании, которые имеют легальное подключение к вычислительной сети компании. Целью такого рода нарушителей является передача информации за пределы автоматизированной системы с целью ее последующего несанкционированного использования — продажи, опубликования ее в открытом доступе и т. д. Данный нарушитель является лицом или группой лиц, которая осуществляет попытки проведения противоправных действий против объектов информационной безопасности, самостоятельно разрабатывая методы и средства реализации атак и проводя атаки. Также предполагается, что данный нарушитель является высококвалифицированным специалистом в области перехвата информации, разработки и эксплуатации программного обеспечения и технических средств. Данный нарушитель не имеет доступа к аппаратной части компьютера внутри системного блока и его системе электропитания. Основные угрозы, исходящие от нарушителя:

· нарушение работоспособности локально-вычислительной сети;

· навязывание ложной информации;

· загрузка операционной системы с внешних носителей.

Рассмотрим данные угрозы подробнее.

Под первой угрозой подразумевается вывод из работоспособного состояния локально-вычислительной сети между атакуемой машиной и сервером службы безопасности. Это может быть разрыв сетевого соединения, имитация неисправности сетевого оборудования, перенаправление информационного трафика, идущего от атакуемой машины к серверу службы безопасности, атака типа «отказ в обслуживании» с целью создания ситуации временной недоступности услуг сети связи.

Под второй угрозой подразумевается отправка заведомо ложной информации с атакуемой машины на сервер службы безопасности.

Под третьей угрозой подразумевается то, что нарушитель может произвести загрузку с внешних носителей своей операционной системы, в которой нет соответствующих систем защиты.

Полностью модель нарушителя представлена в [5].

Для решения проблемы защиты от временного снятия контроля за атакуемой машиной, с учетом этой модели нарушителя, нами предлагается использовать специально разработанный канал передачи сигналов оповещения.

Основными требованиями при разработке канала были:

· гарантированная передача сигналов оповещения о противоправных действиях пользователя на всем протяжении работы компьютера;

· скорость передачи данных не должна позволить использовать его как канал утечки информации;

· передача сигналов должна происходить только в пределах организации;

· канал не должен требовать создания новой среды передачи сигналов;

· формирование сигнала оповещения при попытке загрузки ОС с внешних носителей.

Канал передачи сигналов оповещения, разработанный в [5] с учетом вышеперечисленных требований, позволяет закрыть уязвимости, присущие рассмотренным системам комплексной защиты информации от утечек.

В настоящее время ведется активная работа по вопросам реализации отдельных компонентов системы.

СПИСОК ЛИТЕРАТУРЫ:

1. Современные IT-угрозы и IT-решения защиты. URL: http://www.searchinform.ru/main/full-text-search-information-security-article.html?art=211.
2. Защита информации и бизнеса от инсайдеров 2007. URL: http://www.cnews.ru/reviews/free/insiders2007/articles/negligence.shtml.
3. *Сердюк В. А., Шарков А. Е.* Защита информационных систем от угроз «пятой колонны» // PCWeek. 2003. № 34.
4. Как правильно внедрить DLP-систему? URL: http://www.cnews.ru/reviews/index.shtml?2009/03/24/341782_1.
5. *Мамаев А. В.* Разработка системы передачи сигналов оповещения по сети электропитания ЭВМ для защиты от внутреннего нарушителя. М.: МИФИ, Дипломная работа. 2009.