Хошаба А.М.,
кандидат технических наук, доцент,
доцент кафедры защиты информации
Винницкого национального технического университета
Романюк А. Н.,
доктор технических наук, профессор,
первый проректор Винницкого национального технического университета

ПРОБЛЕМЫ И РЕШЕНИЯ ВНЕДРЕНИЯ СЛУЖБ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В КОМПЮТЕРНЫХ СИСТЕМАХ И СЕТЯХ

В статье изложены основные проблемы безопасности информационных ресурсов в компьютерных системах и сетях, показаны наиболее существенные способы их решения. Подробно рассмотрены основные аспекты внедрения служб безопасности и реализуемые типы атак на компьютерную систему и сети. Описываются взаимодействия основных служб безопасности информационных ресурсов в компьютерных системах и сетях внутри компании.
Ключевые слова: *защита информации, проблемы защиты информации, служб безопасности информационных ресурсов, компьютерные системы, компьютерные сети, компьютерные атаки.*

У статті викладені основні проблеми безпеки інформаційних ресурсів в комп'ютерних системах і мережах, показані найбільш суттєві способи їх вирішення. Докладно розглянуті основні аспекти впровадження служб безпеки і реалізації різних типів атак на комп'ютерну систему і мережі. Описуються взаємодії основних служб безпеки інформаційних ресурсів в комп'ютерних системах і мережах всередині компанії.
Ключові слова: *захист інформації, проблеми захисту інформації, служб безпеки інформаційних ресурсів, комп'ютерні системи, комп'ютерні мережі, комп'ютерні атаки.*

Введение. Использование основных механизмов информационной безопасности не дает стопроцентную гарантию защиты информации или компьютерных систем. Одноко, реализация высокой степени защиты вполне реально, хотя концепции, лежащие в ее основе, сложны. В общем случае информационная безопасность представляет собой систему, позволяющую: выявлять уязвимые места организации; определять опасности, угрожающие структурным подразделениям компании; использовать специальные методы решения проблем безопасности. Используя основные концепции информационной безопасности удае-

тся предотвращать несанкционированные действия и злоупотребления по изменению сведений, фактов, данных или аппаратных средств либо отражать атаки отказа в обслуживании.

Проблемы служб безопасности информационных ресурсов в компьютерных системах и сетях. До настоящего времени не до конца разработанным является процесс сертификации компьютерных систем и сетей, подтверждающий обеспечиваемую безопасность. Для большинства предлагаемых решений информационные технологии слишком быстро опережают время. Так, лабораторией техники безопасности США (Underwriters Laboratory) предлагалась концепция безопасности, согласно которой необходимо создать центр сертификации, удостоверяющий безопасность различных программных продуктов. В случае совершения проникновения в компьютерную систему подробно рассматривались причины и решения конкретных инцидентов.

При этом, поднимались вопросы связанные с програмными продуктами и решениями относительно времени их использования: устаревания сертификатов и повторный пересмотр сертификатов качества защиты информационных ресурсов. К следующей проблеме относилось принятие решение относительно скомпрометировашей системы: построение заново или изменение структуры (реинженеринг)?

Известные методы решения проблемы служб безопасности информационных ресурсов в компьютерных системах и сетях. Практикой показано что нельзя полагаться на один вид защиты для обеспечения безопасности информации так как информационная безопасность не обеспечивает абсолютную защиту и носит характер предупредительных действий. Такие действия позволяют защитить информацию и оборудование от угроз и использования их уязвимых мест. Не существует и единственного программного продукта, реализующего все необходимые способы защиты для компьютерных систем и сетей. Определяющим фактором решения проблемы безопасности информационных ресурсов в компьютерных сетях является комплексный подход в использовании наиболее эффективных средств антивирусного программного обеспечения,

управления доступом к информационным ресурсам компьютерных систем и сетей, использования межсетевых экранов.

Антивирусное программное обеспечение является неотъемлемой частью надежной программы безопасности. При его правильной настройке значительно уменьшается риск воздействия вредоносных программ. Однако никакая антивирусная программа не защитит организацию от злоумышленника, использующего для входа в систему законную программу, или от легального пользователя, пытающегося получить несанкционированный доступ к файлам. Поэтому, компьютерная система в пределах организации должна ограничивать доступ к информационным ресурсам, идентифицируя пользователя, который входит в систему.

При правильной настройке системы, установке необходимых разрешений в доступе для легальных пользователей существует ограничение на использование файлов. Однако система управления доступом не обеспечит защиту, если злоумышленник через уязвимые места получит доступ к файлам как администратор. Такие действия будут расцениваться системой как легальные действиями администратора.

К еще одному действенному способу решения проблемы внедрения служб безопасности информационных ресурсов в компьютерных системах использование межсетевых экранов. Межсетевой экран (firewall) - это устройство управления доступом, защищающее внутренние сети от внешних атак. Оно устанавливается на границе между внешней и внутренней сетью. Правильно сконфигурированный межсетевой экран является важнейшим устройством защиты. Однако он не сможет предотвратить атаку через разрешенный канал связи. Например, при разрешении доступа к веб-серверу с внешней стороны и наличии слабого места в его программном обеспечении межсетевой экран пропустит эту атаку, поскольку открытое веб-соединение необходимо для работы сервера. Межсетевой экран также не защитит от внутренних пользователей, поскольку они уже находятся внутри системы.

Внедрение служб информационной безопасности. Службы информационной безопасности компании являются защитой базового уровня, которые используются для противостояния атакам. Функционироваине каждой из этих служб направлена на борьбу с определенным типом атак.

Особенности использования служб информационной безопасности в компьютерных системах и сетях зависят от уровня оценки риска в конкретной организации и планирования системы безопасности. Знание базовых требований к безопасности компании позволяет эффективно использовать соответствующие службы для противостояния известным атакам.

Служба конфиденциальности обеспечивает сохранность секретной информации. К основным функциям службы относят контроль доступа к информации только аутентифицированных легальных пользователей. Ее надежная работа зависит от службы обеспечения идентификации и однозначного определения подлинности лиц. Выполняя эту функцию, служба конфиденциальности ограждает компьютерню систему и сети от атак доступа.

Служба обеспечения целостности данных отвечает за правильностью структуры и содержания информации. При должном уровне организации безопасности компании, эта служба дает пользователям уверенность в том, что информация является достоверной. Подобно службе конфиденциальности, служба обеспечения целостности должна работать совместно со службой идентификации для осуществления надежной проверки подлинности. Данная служба обеспечивает защиту от атак модификации.

Служба обеспечения доступности информации поддерживает готовность компьютерных систем и сетей к работе приложений и сервисов. Эта служба также должна обеспечивать эффективную передачу информации между конечными пунктами или компьютерными системами в локальных или корпоративных компьютерных сетях.

Про службу идентификации часто забывают, когда речь идет о безопасности. Главная причина недостаточного внимания к ней в том, что сама по себе эта служба не позволяет предотвратить атаки на компьютерные системы или

сети. К ее основной функции относится обеспечение совместной работы с другими службами безопасности информационных ресурсов компьютерных систем и сетей.

Выводы

1. Использование информационной безопасности не обеспечивает абсолютную защиту компьютерных систем и сетей компании и носит характер предупредительных действий. Реализация высокой степени защиты компьютерных систем и сетей компании является важным, сложным и осуществимым мероприятием.

2. Существуют проблемы использования и внедрения служб информационной безопасности которые в первую очередь связаны с сертификацией программных продуктов и систем.

3. При внедрении служб безопасности информационных ресурсов в компьютерных системах и сетях компании должно учитываться особенности их совместной работы.

Литература

1. Гафнер В.В. Информационная безопасность: учеб. пособие[1]. – Ростов на Дону: Феникс, 2010. - 324 с.

2. Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. В 2-х томах. Том 1. — Угрозы, уязвимости, атаки и подходы к защите. — М.: Горячая линия - Телеком, 2006. — 536 с. Том 2. — Средства защиты в сетях. — М.: Горячая линия - Телеком, 2008. — 560 с.

3. Малюк А.А. Теория защиты информации. — М.:Горячая линия - Телеком, 2012. — 184 с.

4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2008. — 544 с.