Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.451.2

Шилов

Артём Сергеевич

Методика безопасного конфигурирования операционных систем семейства Windows

АВТОРЕФЕРАТ

магистерской диссертации на соискание степени магистра технических наук

по специальности 1-98 80 01 «Методы и системы защиты информации, информационная безопасность»

Научный руководитель

Бойправ О.В.

к.т.н., доцент

Минск 2019

ВВЕДЕНИЕ

Стремительное развитие информационных технологий привело к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Однако с развитием информационных технологий возникают и стремительно растут риски, связанные с их использованием, появляются новые угрозы.

Одним из главных инструментов для реализации конкретных информационных технологий являются информационные системы, задача обеспечения безопасности которых является приоритетной, так как от сохранения конфиденциальности, целостности и доступности информационных ресурсов зависит результат деятельности информационных систем. Операционная система является важнейшим программным компонентом любой вычислительной машины, поэтому от уровня реализации политики безопасности в каждой конкретной операционной системе во многом зависит и общая безопасность информационной системы.

Данная работа посвящена разработке методик обеспечения безопасности операционных систем семейства Windows путем конфигурации их параметров, в зависимости от предъявляемых требований к безопасности.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Цель и задачи проводимых исследований

Целью работы является исследование средств безопасности в операционных системах семейства Windows и разработка принципов конфигурирования этих средств в зависимости требований к степени защищенности информационной сети, в которой используются указанные системы.

Для достижения поставленной цели необходимо решить следующие задачи.

1 Изучить средства безопасности в операционных системах семейства Windows.

2 Проанализировать основные подходы для обеспечения безопасности операционных систем семейства Windows.

3 Определить оптимальный перечень средств безопасности операционных систем семейства Windows, а также разработать подходы к их конфигурированию.

Связь работы с приоритетными направлениями научных исследований

Тема диссертационной работы соответствует пункту 13 «Безопасность человека, общества и государства» приоритетных направлений фундаментальных и прикладных научных исследований Республики Беларусь на 2016–2020 годы, утвержденных Постановлением Совета Министров Республики Беларусь от 12.03.2015 г. № 190.

Апробация результатов диссертации

Основные результаты диссертации докладывались и обсуждались на 54-й и 55-й научных конференциях аспирантов, магистрантов и студентов БГУИР (г. Минск, 23–27 апреля 2019 г.; 22–26 апреля 2019 г.), XVI и XVII Белорусско-российских научно-технических конференциях (г. Минск, 5 июня 2018 г.; 11 июня 2019 г.)

КРАТКОЕ СОДЕРЖАНИЕ РАБОТЫ

Диссертация состоит из введения, трех глав, заключения и библиографического списка. Общий объем диссертации 81 страница, 16 наименований в библиографическом списке.

Во введение приводится обоснование актуальности работы.

Первая глава носит обзорный характер. В ней проводится анализ архитектур современных операционных систем, рассмотрены особенности UNIX-подобных операционных систем и операционных систем семейства Windows.

Вторая глава посвящена анализу настроек безопасности и средствам обеспечения безопасности операционных систем семейства Windows, описаны параметры системы, влияющие на безопасность, настройки этих параметров по умолчанию и проведён анализ программного обеспечения, используемого для обеспечения безопасности операционных систем семейства Windows.

В третьей главе разработаны методики конфигурирования, заключающиеся в настройке параметров локальных групповых политик с целью усиления безопасности. Предложенная конфигурация «Enterprise» предназначена для рабочих мест корпоративной сети и направлена на снижение влияния действий пользователей и ПО на систему. конфигурации «High Security» предназначена для устройств с повышенным требованием к безопасности. Эта конфигурация должна еще больше ограничивать влияние пользователей и приложений на систему, в сравнении с конфигурацией «Enterprise», больше внимания уделяется аудиту событий безопасности и защите от внедрения вредоносного кода. Проведён анализ влияния описанных конфигураций на производительность системы. Кроме того, был описан алгоритм проверки выполнения настроек при помощи специализированного ПО Microsoft Security Compliance Manager.

В заключении сформулированы основные результаты диссертации.

ЗАКЛЮЧЕНИЕ

Современные ОС семейства Windows, используемые для серверов и персональных компьютеров, основаны на архитектуре Windows NT. Они функционируют по схожим принципам, имеют гибридное ядро и общие решения вследствие закрытости системы. В состав ОС входит ПО, выполняющее функции защиты информации, и широкий набор настроек безопасности. Проблема заключается в надлежащем выборе параметров безопасности и режимах работы защитного ПО, т.к. конфигурация системы по умолчанию не пригодна для обеспечения информационной безопасности. В рамках данной работы, путём анализа встроенных средств защиты, были разработаны две методики конфигурирования операционных систем семейства Windows, применяющиеся в зависимости от строгости требований информационной безопасности в отношении конкретной системы. Было проанализировано влияние предложенных конфигураций на быстродействие системы и сделан вывод, что их использование незначительно увеличивает расход оперативной памяти и не ведёт к серьёзному снижению производительности.

СПИСОК ПУБЛИКАЦИЙ СОИСКАТЕЛЯ

1–А Шилов, А. С. Подходы к безопасному конфигурированию операционных систем семейства Windows/ А. С. Шилов, О. В. Бойправ // Технические средства защиты информации : тез. докл. XVI Белорусско-российской науч.-техн. конф. Минск, 5 июня 2018 г. / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2018. – С. 100–101.

2–А Шляхтич, А. Н. Программное обеспечение для построения защищенных виртуальных сред / А. Н. Шляхтич, А. С. Шилов // Технические средства защиты информации : тезисы докладов XVII Белорусско-российской науч.-техн. конф. Минск, 11 июня 2019 г. / редкол. : Т. В. Борботько [и др.]. – Минск : БГУИР, 2019. – С. 79.