эффективности защиты можно достичь, только используя несколько средств одновременно, а это говорит о том, что ни одно средство не может полностью обеспечить необходимую степень защиты. Выбирать эти средства защиты нужно под конкретный процесс, при этом контроль доступа становится важнейшим элементом защиты компьютера и информации. Информация необходима миллионам людей ежедневно, поэтому её защита заключается не в ограничении доступа к ней, а в его разграничении и защите от вредоносных воздействий.

Цель работы заключается в исследовании и реализации алгоритма защиты от вредоносных программ на основе контроля доступа к файлам.

Самыми распространенными методами к защите от вредоносных программ на основе контроля доступа к файлам являются:

• Методы контроля доступа с механизмами ограничения как: идентификация и аутентификация.

• При входе пользователя в систему производится первый шаг идентификации.

Далее пользователь запускает процессы, которые задают потоки, осуществляющие обращение к защищенным ресурсам. Все процессы в системе и потоки нацелены на защиту пользователя, от имени которого был произведен запуск процессов. Для идентификации контекста защиты процесса или потока используется объект, называемый маркером доступа (accesstoken), который содержит информацию по безопасности.

В состав защиты данных входит информация, описывающая привилегии, учетные записи и группы, сопоставленные с процессом и потоком. При регистрации пользователя в системе создается начальный маркер, определяющий пользователя, который входит в систему, и сопоставляющий его с процессом оболочки, применяемой для пользовательской регистрации. Все программы, запускаемые пользователем, получают копию этого маркера.

Методы контроля доступа, основанные на разграничении доступа, различающиеся способами идентификации субъекта и объекта доступа, а также методами задания и хранения правил (политики) разграничения доступа.[1]

Избирательное управление. Этот метод задает каждой паре (субъект – объект) перечисление допустимых типов доступа (редактирование, просмотр, добавление и т.д.), для тех типов, которые являются санкционированными (разрешенными) для данного субъекта (индивида или группы индивидов) к данному ресурсу (объекту).

Мандатный метод контроля доступа. В этом методе все уровни доступа или мандаты присваиваются пользователям.[2]

Управление доступом по принципу присвоения ролей. Образование ролей призвано определить четкие и понятные для пользователя компьютерной системы правила разграничения доступа к данным.

Для защиты от вредоносных программ обычно применяют комплекс подходов, сочетающий два и более метода, при этом необходимо соотносить важность информации и сложность защиты, так как использование модульных методов для защиты маловажной информации приводит к напрасной трате как времени, так и затрате машинных и человеческих ресурсов.

В результате исследования предметной области можно сделать вывод, что защита от вредоносных программ на сегодняшний день является самой актуальной проблемой, потому как развитие информационных систем не стоит на месте. Любая важная информация нуждается в защите. На пути решения (разработки) необходимо исследовать все достоинства и недостатки каждого их методов по защите информации. Так же учитывать уже существующие разработки по защите информации от вредоносных программ, максимально модернизировать систему, расширить функциональные возможности, улучшить качество реализации, повысить степень защиты, избавиться от весомых недостатков системы существующих на данный момент.

Список литературы

1. Щеглов А.Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем: Учебное пособие.– СПб.: Университет ИТМО, 2014. – 95 с.

2. Щеглов К.А., Щеглов А.Ю. Реализация метода мандатного доступа к создаваемым файловым объектам // Вопросы защиты информации. – 2013. – Вып. 103. – № 4. – С. 16-20.

ИСПОЛЬЗОВАНИЕ МЕТОДОВ ВИЗУАЛИЗАЦИИ ДЕКОМПОЗИРОВАННОЙ ОНТОЛОГИИ ПРЕДМЕТНОЙ ОБЛАСТИ

Савицкий И.В., Рыбанов А.А.

Волжский политехнический институт, филиал ВолгГТУ, Волжский, e-mail: savickijugor@gmail.com

На сегодняшний день информация является одним из ключевых ресурсов для человека. Для описания экспертных знаний в различных информационных системах широко применяются онтологии. Однако, чем большее количество знаний описывается в онтологии, тем труднее пользователю её понять.

Одним из лучших способов представления онтологии является её визуализация. На данный момент существует множество программных средств, которые способны визуализировать онтологии. Однако, если в онтологии присутствуют знания, которые трудно описать в виде элемента графа, большинство программных средств не смогут их отобразить. Также данные средства почти не учитывают при визуализации смысл представленных в онтологии понятий и отношений, к тому же в процессе визуализации практически не происходит декомпозиции онтологии, из-за чего визуализация может создать трудночитаемую схему, что отрицательно сказывается на понимании пользователем информации.

Целью данной работы является исследование методов визуализации алгоритма декомпозиции онтологии предметной области

Основные задачи исследования:

1. Анализ современных технологий визуализации онтологий предметных областей.

2. Изучение алгоритмов декомпозиции онтологий предметных областей.

3. Разработка модели декомпозиции онтологии предметной области

4. Разработка тестового варианта программы-визуализатора онтологий предметных областей

5. Экспериментальная оценка предлагаемых методов.

Для экспериментальной оценки полученных теоретических результатов в качестве практических результатов планируется разработка программы. В итоге получится программа-визуализатор онтологии предметной области, перед визуализацией проводящая процесс декомпозиции над онтологией.

Список литературы

1. Ломов П.А., Шишаев М.Г. Визуализация OWL-онтологий на основе когнитивных фреймов.