РЕФЕРАТ

Объем ВКР 83 страницы, 39 рисунков, 8 таблиц, 49 источников.

Ключевые слова: ERP-система, сетевая атака, эпидемический процесс, деструктивные воздействия, моделирование, риск-анализ.

Объектом исследования является ERP-система, которая может подвергнуться сетевой атаке.

Предметом исследования является организация защиты ERP-систем от сетевых атак.

Целью исследования является разработка методов и моделей организации защиты ERP-систем от сетевых атак.

Для достижения поставленной цели, необходимо решить следующие задачи:

- всестороннее исследование ERP-систем из чего они состоят и как устроены;
- вероятностный анализ сетевых атак на ERP-системы и анализ поведения систем после деструктивного воздействия;
- разработка методов и моделей организации защиты ERP-систем от сетевых атак и их деструктивного воздействия.

Новизна результатов:

1) алгоритмизированная дискретная микромодель эпидемического процесса учитывает такую структурную особенность, как динамическое развитие ERP-систем, благодаря чему более адекватно отражаются процессы, протекающие в ERP-системах при эпидемии;

2) формализована модель межсетевого распространения контента пользователями в ERP-системах;

3) проведено моделирование и анализ эпидемических процессов в ERP-системах с различными структурными свойствами;

Практическая ценность работы заключается в том, что:

– алгоритмизированная дискретная микромодель эпидемического процесса позволяет учитывать динамическое развитие ERP-систем, что позволяет провести ее анализ, приближенный к реальности;

– формализованная модель распространения контента пользователями, зарегистрированными и использующими одновременно ERP-систему, может быть в дальнейшем внедрена в программный комплекс, что позволит более адекватно отражать процессы, протекающие в информационных сетях при эпидемическом процессе;

– выработанные рекомендации по защите ERP-систем и управлению структурной живучестью при угрозе сетевых атак, при практическом применении позволяют своевременно реагировать на деструктивные воздействия и распространение нежелательной информации внутри системы, и блокировать узлы-распространители, не нарушая при этом структурной целостности ERP-системы во время;

– запрограммированная дискретная микромодель эпидемического процесса позволяет учитывать динамическое развитие ERP-систем, что может быть использовано для проведения более глубокого и близкого к реальности моделирования эпидемического процесса.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Сегодня главным условием стабильного функционирования системы становится совершенствование процедур организационного управления, в том числе и при использовании информационных технологий. В частности, на базе современных компьютерных технологий создано поколение систем управления, именуемое ERP (Enterprise Resource Planning — планирование ресурсов предприятия, то есть системы управления ресурсами) [1-2]. Компоненты ERP-системы содержат критичную для деятельности компании информацию, конфиденциальность, целостность и доступность которой имеют огромное значение. Именно по этой причине каждое звено ERP-системы должно быть надежно защищено, так как негативное внешнее или внутреннее воздействие на любой ее участок может иметь самые серьезные последствия для деятельности всей компании. ERP-системы наиболее востребованы в крупных организациях и отраслях, где требуется координировать работу большого количества подразделений и умело планировать использование всех имеющихся ресурсов [3-4]. Современные ERP-системы обеспечивают выполнение всех самых основных функций и процессов предприятия. В их основе лежит принцип создания единого хранилища данных, содержащего всю корпоративную информацию и обеспечивающего одновременный доступ к ней любого сотрудника, наделённого соответствующими полномочиями. Поскольку ERP-система активно участвует практически во всех информационных процессах компании и осуществляет хранение, обмен, передачу и обработку данных, то она часто становится целью атаки злоумышленника, как внутреннего так и внешнего, что в свою очередь несет риск для предприятия в целом [5]. Например, кража конфиденциальной информации или остановка критичных бизнес-процессов может привести к существенным финансовым и репутационным потерям. Анализ источников показывает, что ERP-системы обладают весьма сложной архитектурой, объединяющей в себе различные технологии, такие как серверы приложений, базы данных, межплатформенное программное обеспечение, веб-сервер, операционные системы, системы управления идентификаторами [6-7]. Такая сложность создает

дополнительные угрозы с точки зрения информационной безопасности, которые могут возникать как на этапах проектирования и разработки ERP-системы, так и на этапах внедрения и эксплуатации. Исходя из вышесказанного, можно наблюдать следующие **противоречия** между:

- ростом частоты и величины возникающих ущербов от реализации сетевых атак и недостаточным уровнем защищенности ERP-систем от данного вида деструктивных воздействий;
- потребностью в научно обоснованных методах риск-анализа субъектов сетевых атак ERP-систем и готовностью науки предоставить данные методы для эффективного;
- значимостью внедрения средств защиты информации в ERP-системах и последующей их настройки в целях снижения рисков успеха реализации сетевых атак различного характера на серверы, функционирующие в составе атакуемых систем.

Степень разработанности темы исследования. Тема исследования ERP-систем в настоящее время является популярной и свидетельствует об этом [8-9]. Уже было произведено немало исследований касательно не только самих ERP-систем, но и деструктивных воздействий, которым они подвергались благодаря сетевым атакам.

К настоящему времени было уже представлено немало работ, которые в разной степени затрагивают и описывают сетевые атаки в ERP-системах, но в них не используется моделирование сетевых атак на ERP-системы.

Представленные выше источники позволяют говорить о том, что повышение защищенности систем, которые представляют из себя ERP-системы, и процессов, которые в них протекают, является одним из приоритетных направлений исследования и остается актуальной на протяжении довольно большого временного периода [10]. Моменты, относящиеся к созданию методического, информационного, алгоритмического и программного обеспечения дискретного вероятностного моделирования процессов, имеющих эпидемический характер и протекающих в ERP-системах, с возможностью составления прогнозов разного рода относительно

заданной информации, распространяемой в заданной среде, являются довольно мало реализованными, но при этом имеют немалую научную и даже практическую ценность.

Объектом исследования является ERP-система, которая может подвергнуться сетевой атаке.

Предметом исследования является организация защиты ERP-систем от сетевых атак.

Целью исследования является разработка методов и моделей организации защиты ERP-систем от сетевых атак.

Для достижения поставленной цели, необходимо решить следующие **задачи:**

- всестороннее исследование ERP-систем из чего они состоят и как устроены;
- вероятностный анализ сетевых атак на ERP-системы и анализ поведения систем после деструктивного воздействия;
- разработка методов и моделей организации защиты ERP-систем от сетевых атак и их деструктивного воздействия.

ERP-система – это система планирования ресурсов предприятия по всем основным направлениям его деятельности [11].

Использование полнофункциональной единой системы управления ресурсами компании может дать огромные преимущества предприятию в организации эффективного управления компанией, увеличении быстроты реакции на изменения внешней среды, повышении качества обслуживания клиентов.

Внедрение ERP-системы на предприятии не только помогает повысить степень автоматизации отдельных процессов, но и провести реинжиниринг самих этих процессов. В результате такого внедрения стандартизируется подавляющее большинство операций, значительно растет управляемость организации, повышается степень ее информационной открытости.

Основными понятиями в структуре любой ERP-системы являются понятия модели объекта и процесса. Суть внедрения системы на предприятии состоит в

установлении соответствия между этими параметрами системы и элементами и процессами реальной организации [12-13].

Взаимодействие с ERP-системой осуществляется путем ввода данных и получения отчетов. Ввод данных организуется таким образом, чтобы исключить любое дублирование и обеспечить должный уровень контроля за правильностью ввода для исключения возможных ошибок оператора. Выходные данные могут предоставляться как в виде стандартных отчетов, так и результатов специальных запросов пользователя. Для удобства использования отчеты размещаются в корпоративной или глобальной сети, а также интегрируются в различные пользовательские приложения [14].

Новизна результатов:

1) алгоритмизированная дискретная микромодель эпидемического процесса учитывает такую структурную особенность, как динамическое развитие ERP-систем, благодаря чему она не имеет аналогов и более адекватно отражает процессы, протекающие в ERP-системах при сетевых атаках;

2) впервые формализована модель межсетевого распространения контента пользователями в ERP-системах;

3) проведено моделирование и анализ эпидемических процессов в ERP-системах с различными структурными свойствами и выработаны методы защиты для ограничения пользователя, которые отличаются эффективностью, быстродействием и отказоустойчивостью от имеющихся аналогов.

Практическая ценность работы заключается в том, что:

– алгоритмизированная дискретная микромодель эпидемического процесса позволяет учитывать динамическое развитие ERP-систем, что позволяет провести ее анализ, приближенный к реальности;

– формализованная модель распространения контента пользователями, зарегистрированными и использующими одновременно ERP-систему, может быть в дальнейшем внедрена в программный комплекс, что позволит более адекватно отражать процессы, протекающие в информационных сетях при эпидемическом процессе;

– выработанные рекомендации по защите ERP-систем и управлению структурной живучестью при угрозе сетевых атак, при практическом применении позволяют своевременно реагировать на деструктивные воздействия и распространение нежелательной информации внутри системы, и блокировать узлы-распространители, не нарушая при этом структурной целостности ERP-системы во время;

– запрограммированная дискретная микромодель эпидемического процесса позволяет учитывать динамическое развитие ERP-систем, что может быть использовано для проведения более глубокого и близкого к реальности моделирования эпидемического процесса.

Методы исследования. Для решения поставленных задач в работе используются методы системного анализа, математического анализа, теория графов и методы математического моделирования.

ЗАКЛЮЧЕНИЕ

В результате проделанной работы было осуществлено исследование параметрического и структурного содержания ERP-систем в контексте вероятности распространения деструктивного контента и сетевых атак на них. Данные исследования послужили основой при составлении выводов по корпоративным информационным сетям.

Была осуществлена алгоритмизация динамического развития ERP-систем для последующего ее использования в процессе моделирования эпидемического процесса в программном обеспечении, получаемом в результате работы.

Был проведен анализ влияния параметрического и структурного содержания ERP-систем с целью поиска вероятности распространения деструктивного контента. Также были выработаны рекомендации для борьбы с сетевыми атаками и управлением структурной живучестью для исследуемых систем.

Полученные в результате выполнения данной работы алгоритмы моделирования сетевых атак на ERP-системы были реализованы в разрабатываемом программном комплексе для более приемлемого и точного моделирования эпидемического процесса.

Результат, который был получен в выполненной работе, может стать основой для дальнейшего развития ERP-систем в различных информационных сферах. Кроме того, остался ряд направлений, в которых все еще возможно усовершенствовать как саму ERP-систему, так и разрабатываемый программный комплекс. Представим отдельно перспект

Перспективные направления развития. Следует правильно применить типовые структуры, чтобы сделать реализуемые операции более эффективными и оптимальными. Отладить полученное программное обеспечение, исправить неточности, ошибки как полученные в результате программирования, так и те, которые получатся вследствие неточной разработки теоретической модели. Это следует сделать как для учета динамического изменения ERP-систем, так и для их защиты от сетевых атак.