ВВЕДЕНИЕ

Актуальность исследования. Информация является одним из важнейших активов любой организации, поэтому они должны быть соответствующим образом защищены. Информация объединяет системы безопасности, операций и внутреннего контроля для обеспечения целостности и конфиденциальности данных, и процедур работы в организации. Доступность информации также важна для организации. Если информация целостна и конфиденциальна, но не доступна для авторизованных пользователей, она считается бесполезной.

Системы планирования ресурсов предприятия (Enterprise resource planning) - это программные системы для управления бизнесом, охватывающие модули, поддерживающие такие функциональные области, как планирование, производство, продажа, маркетинг, дистрибуция, учет, финансы, управление персоналом, управление проектами, управление запасами, обслуживание, транспортировка и электронный бизнес. Архитектура программного обеспечения облегчает прозрачную интеграцию модулей, обеспечивая постоянный поток информации между всеми функциями внутри предприятия. Внедрение ERP позволяют компаниям внедрять единую интегрированную систему путем замены своих несовместимых устаревших информационных систем. ERP состоит из коммерческого пакета программного обеспечения, который включает бесшовную интеграцию всей информации. ERP-системы представляют собой настраиваемые пакеты информационных систем, которые объединяют информационные процессы и функциональные области в организации. Обеспечение той или иной степени защищенности информации необходимо на каждом уровне. При этом выбор механизмов защиты информации на различных уровнях ERP-системы зависит от специфики конкретного проекта и от уровня риска каждой угрозы. Роль оценки риска информационной безопасности в деятельности предприятий очень велика [4]. Полученные значения рисков ИБ необходимы для выработки рекомендаций по снижению уровня риска при использовании ERP-системы, а также принятия эффективных мер по обеспечению ИБ всего предприятия.

Степень проработанности темы исследования. В имеющейся литературе рассмотрены такие вопросы, как:

– классификация, анализ [6], ERP-систем [9];

– построение корпоративной сети с внедренной ERP-системой;

– особенности ERP систем, анализ существующих угроз [11, 12];

– определение вершин и ребер в графе [4, 8];

– угрозы и риски распространения вредоносной информации в корпоративных сетях [10].

Однако, несмотря на большое количество уже существующих работ, связанных с заданной тематикой, остаются не проработанными отличительные особенности процессов распространения информационных эпидемий внутри корпоративных сетей с внедренной ERP-системой.

Исходя из проанализированных источников в ERP-системах наблюдаются следующие противоречия между:

- ростом частоты возникающих угроз от реализации информационных атак и недостаточным уровнем защищенности ERP-систем;
- потребностью в научно обоснованных методах риск-анализа субъектов информационных атак и готовностью науки предоставить данные методы для эффективного их использования;
- значимостью внедрения средств защиты информации в корпоративные сети, в которую внедрены ERP-системы, и последующей их настройки в целях снижения рисков и реализации информационных атак различного характера на главные серверы, и различные ПК пользователей.

Объектом исследования являются ERP-системы и модели оценки информационных рисков.

Предметом исследования являются риски, связанные с информационными атаками на ERP-системы.

Цель исследования состоит в повышении защищенности ERP систем, на основе разработки их моделей, учитывающих конфликтность противоборствующих в них субъектов.

ЗАКЛЮЧЕНИЕ

В результате выполнения выпускной квалификационной работы был проведен всесторонний анализ ERP-систем в целях исследования методов и моделей для предотвращения распространения вредоносного контента.

В первой части данной работы было дано подробное описание и анализ ERP-систем. Проанализированы основные уязвимости данных систем, предложено методы обеспечения безопасности.

Во второй части работы, рассмотрена модель оценки информационных рисков при использовании ERP систем, сделана оценка рисков для ERP систем. Данные методики и ее этапы могут применяться при оценке рисков информационной безопасности ERP-систем. И будут аналогичны для любых организаций, независимо от сферы их деятельности, масштабов, уровня организационной зрелости.

В третьей части работы промоделирована корпоративная сеть с внедренной в нее ERP-систему. Сформирована модель инфицирования сети, проанализированы модели эпидемий для трех случаев. Предложены рекомендации по управлению информационными рисками в ERP-системах.

Результат, который был получен в выполненной работе, может стать основой для дальнейшей оценки и анализа информационных рисков в ERP-системах.