Полозова Екатерина Андреевна, 1-й год обучения

Модель угроз безопасности информации при разработке DLP-систем

Научный руководитель: проф. каф. «ИТиЗИ» к.т.н, доцент, Зырянова Т.Ю.

На данный момент информационная безопасность становится достаточно актуальным, и в тоже время сложным направлением в области безопасности личности, общества, государства. Существует множество проблем, касающиеся защиты информации. И в постоянной гонке угроз информационной безопасности и системы защиты информации от данных угроз очень важно смотреть далеко вперед, определить возможные и невозможные угрозы, проанализировать, структурировать и разработать средство защиты. Стоит вопрос проблемы структуризации угроз, чтобы в дальнейшем на наглядном модели представлялось возможным разработать средство защиты. Областей, направлений информационной безопасности, средств защиты информации очень много. Одно из относительно недавних средств защиты информации, которая постепенно набирает свои обороты – это DLP – системы (предотвращение утечек информации (англ. Data Leak Prevention)). Данные системы имеют достаточной большой набор преимуществ, но имеют и некоторые недостатки, недоработки. Системы DLP защищают от некоторых угроз, но каким образом угрозы структурированы, остаётся под вопросом. Возможно, что решения возникали по мере необходимости и по желаниям клиентов. Но иногда клиент не может видеть вперед и предугадать, какая проблема защиты может возникнуть в дальнейшем. Для этого необходимо разработать модель угроз безопасности информации для DLP-систем, на которую можно опереться при разработке системы защиты информации. В данной работе рассматривается вопрос моделирования угроз безопасности DLP-систем. В открытых источниках нет конкретных моделей. Поэтому, надеюсь, что эта работа поможет специалистам по защите информации и другим специалистам по-новому взглянуть на DLP-системы, модели угроз и системы защиты информации от несанкционированного доступа.

Целью исследования является разработка модели угроз безопасности информации при разработке DLP-систем.

Задачи исследования:

* провести системный анализ внутренних угроз информационной безопасности предприятия;
* разработать алгоритм определения общей модели актуальных угроз при разработке DLP-систем;
* разработать алгоритм определения частной модели актуальных угроз при разработке и внедрении DLP-системы в конкретной организации;

Практическая значимость работы определяется возможностью использования предложенной модели угрозы информационной безопасности, алгоритма и методики определения угроз для практической реализации DLP-систем.