УДК 004.021

РАЗРАБОТКА МЕТОДИКИ МИНИМИЗАЦИИ УРОВНЯ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ НЕСАНКЦИОНИРОВАННОМ ИЗМЕНЕНИИ PE-ФАЙЛОВ НА ОСНОВЕ ЛИНЕЙНОГО ПРОГРАММИРОВАНИЯ

Березин Г.В. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)
Научный руководитель – к.т.н., доцент Левко И.В.
(федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

В данном докладе рассматривается возможность уменьшения уровня рисков, связанные с изменением исполнительных файлов, которые используются в рамках предприятия. В частности, эту проблему предлагается решить путем применения новой методики на основе линейного программирования.

Введение. В настоящее время почти все предприятия активно используют в своих сетях сторонние приложения и программы, направленные на реализацию задач предприятия. Доверяя скачиваю лицензионного программного обеспечения, сотрудники теряют бдительность в обеспечении безопасности своего аппаратного комплекса, устанавливая потенциально опасный продукт, который может быть скомпрометирован злоумышленниками. В итоге это приводит к возможной утечке данных, хранящихся на вычислительных машинах предприятия, которые могут содержать конфиденциальную информацию, распространение которой влечет за собой как репутационный, так и финансовый ущерб предприятию. Чтобы избежать подобных последствий, эксперты информационной безопасности часто используют крайние меры, полностью запрещая какие-либо самостоятельные действия по скачиванию и установке стороннего программного обеспечения. Это сказывается на финансовой составляющей поддержки информационной безопасности на предприятии, что так же не является лучшим решением. В результате можно наблюдать, что почти все кампании выбирают крайности в обеспечении информационной безопасности по установке и скачиванию исполняемых (PE) файлов.

Основная часть. Вышеописанные проблемы предлагается решить путем создания методики по минимизации уровня рисков при несанкционированном изменении PE-файлов на основе линейного программирования. В этапах данной методики рассматриваются такие аспекты как: пути внедрения измененного файла в локальную вычислительную сеть, составление категорий возможных угроз, произведение выбора способа оценки рисков информационной безопасности и дальнейшая выработка рекомендации по минимизации уровня рисков на предприятии.
Отличительной чертой методики является использование задач по оптимизации в синтезе с организационными мероприятиями, направленные на обеспечение информационной безопасности, в то время как большинство методов полагаются на мнение экспертов.
Точные математические расчеты позволят выбрать наиболее правильную тактику по обеспечению информационной безопасности, направленной на использование сторонних приложений и программ.

Выводы. Разработка данной методики и её применение на предприятиях разрешат проблему частой утечки конфиденциально важной информации через сторонние приложения. А потенциальная минимизация как ущерба, так и финансовых затрат позволит популяризировать методику в молодых кампаниях.

Березин Г.В. (автор)

Левко И.В. (научный руководитель)