

В. В. Медведев, ООО «Доктор Веб», Москва, v.medvedev@drweb.com

Возможность выработки требований к системе защиты от вредоносных программ

Несмотря на то что вредоносные программы, а также средства защиты от них существуют уже несколько десятилетий, до сих пор не имеется правильных определений понятий «вредоносная программа» и «антивирус». В данной работе делается попытка выработки требований к анти-вирусной системе защиты, что позволит компаниям и частным пользователям реализовывать надежную защиту от современных угроз.

Ключевые слова: термины и определения, антивирус, вредоносная программа, информационная безопасность, стандарты, рекомендации.

Введение

Как ни странно, несмотря на огромное количество различных стандартов в области информационной безопасности, успешную деятельность ряда международных компаний и организаций, до сих пор единых определений в данной области не выработано. Нет даже такого базового определения, как вредоносная программа.

Отсутствие правильной терминологии дезориентирует как ИТ-специалистов, так и частных пользователей. Так, неверное понимание задач и возможностей антивируса не позволяет компаниям и организациям правильно оформить требования в ходе закупки и в процессе внедрения защитных мер. Системы защиты, построенные без понимания возможностей продуктов, не могут противостоять криминалитету.

Необходимо отметить, что правильное понимание возможностей и ограничений различных типов систем защиты позволяет оптимально использовать финансовые ресурсы компаний и организаций.

Более того, неверная терминология активно используется мошенниками для продвижения своих «решений».

Данная статья содержит:

- 1) анализ имеющихся терминов и определений в области антивирусной безопасности;
- 2) анализ ряда руководящих документов регуляторов в области антивирусной защи-

ты в отношении возможностей систем защиты, построенных в соответствии с такими документами;

3) рекомендации, которых необходимо придерживаться при выборе систем антивирусной безопасности.

К сожалению, несмотря на огромное количество литературы по теме вредоносных программ, большая ее часть описывает сами вредоносные программы. Более того, имеется литература, содержащая советы, которые могут принести только вред. В ходе подготовки данной статьи автором не обнаружено литературы, посвященной анализу терминов и определений в области антивирусной защиты.

Анализ имеющихся определений термина «вредоносная программа»

Приведем лишь несколько определений из различных источников.

- «Вредоносная компьютерная программа — компьютерная программа либо иная компьютерная информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации»¹.

¹ Уголовный кодекс Российской Федерации. Ст. 273. URL: http://www.pravo.gov.ru/proxy/ips/?docbody=&link_id=1&nd=102041891