УДК 004.49

НЕЧЕТКАЯ МОДЕЛЬ АГРЕССИВНОСТИ ПОЛЬЗВАТЕЛЬСКОЙ ПРОГРАММЫ

Фомичев Д.П.

Аспирант 2 года обучения,

Российский технологический университет (МИРЭА)

e-mail: der_adler@inbox.ru

Аннотация: Рассматриваются вопросы исследования нечеткой модели важного свойства пользовательского программного средства – агрессивности, характеризуемого возможностями по перехвату управления у операционных систем в процессе выполнения отдельных программ или их совокупностей, находящихся в памяти компьютера.
Ключевые слова: программная закладка, агрессивность, разрушающее программное средство, информационная безопасности.

FUZZY MODEL OF AGGRESSIVITY OF THE USER PROGRAM

Fomichev D.P.

Graduate student 2 years of study,

Russian Technological University (MIREA)

e-mail: der_adler@inbox.ru

Abstract: The questions of researching a fuzzy model of an important property of a user software tool — aggressiveness, characterized by the ability to intercept control from operating systems in the process of executing individual programs or their assemblies located in the computer's memory are considered.
Keywords: software bookmark, aggression, destructive software, information security, fuzzy program model.

Анализ современной тенденции проектирования и разработки программных средств (ПС) показывает, что процесс создания программ часто приводит к результату, в функциональном плане отличающемуся:

- повышенными требованиями к ресурсам вычислительных систем;
- способностью производить изменения в вычислительных процессах на системном уровне;
- возможностью доступа к любому ИО системы и операциям над ним.

Кроме того, в геометрической прогрессии увеличивается множество ПС, в которые на начальных этапах проектирования вносятся функции, выполняющие отличную от требуемой задачу, (в том числе, разрушающие функции), вплоть до создания непосредственно разрушающих программных средств (РПС) [1,2]: вирусы, программные закладки и т.п.

Формальное представление возможных ситуаций проявления выше указанных агрессивных свойств программного средства позволяет сформулировать показатели, которые способны повысить точность оценки уровня безопасности программного обеспечения.

Исследования агрессивности программ проводились специалистами до последнего времени в области вирусов и представляли собой попытки описать «опасность» таких разрушающих программных средств [3,4]. При этом, как правило, под степенью опасности вируса понимался потенциально наносимый им вред, который измеряется по некоторой ***n***-балльной шкале. Такой подход на наш взгляд имеет ряд недостатков:

- отсутствие формального описания этих n-уровней опасности вирусов;
- отсутствие показателей и метрик, характеризующих тот или иной уровень опасности вируса;
- неполное представление содержания опасности вируса.

Кроме того, практически любой современный программный продукт можно рассматривать как объект, представляющий опасность для вычислительной системы. Это проявляется и в захвате ресурсов системы для обеспечения его функционирования, и в изменении данных системы и т.д. Таким образом, термин «опасность» или «агрессивность» можно отнести не только к собственно РПС, но и к любому системному или прикладному ПС. Следовательно, необходимо разработать обобщенное описание агрессивных свойств любого программного средства [5].

Свойство агрессивности характеризует степень потенциальных разрушающих воздействий какого-либо объекта.

Агрессивным программным средством будем считать такое ПС, которое имеет хотя бы один агрессивный программный элемент (АПЭ) [2,6]. Степень агрессивности ПС определяется в первую очередь мощностью (М) множества агрессивных программных элементов. Вид этой зависимости может быть определен экспертным путем [7] с последующим уточнением в ходе экспериментов, например, в виде функции принадлежности $\mu = \mu(M)$. Под агрессивным программным элементом будем понимать такой программный элемент,который способен [7,8], при определенных условиях, вызвать модификацию:

– информационных объектов (ИО) вычислительной среды, в том числе других элементов агрессивного ПС (под программным элементом будем понимать логически завершенный участок программы, имеющий один вход и один выход);

– состояния вычислительной среды (характеристики ресурсов вычислительной системы (ВС), параметры вычислительного процесса (ВП) и т.д.).

Свойство агрессивности проявляется в динамике и зависит от характера процессов, активизирующихся в данный момент времени. В остальное время (до момента активизации и после момента их завершения) вычислительную среду или ПС будем считать потенциально агрессивными.

Показатель агрессивности программного средства – понятие, отражающее разрушающие свойства программного средства. Рассмотрим основные показатели агрессивности [9].

Метрика агрессивности ПС –измеряемая количественно характеристика разрушающих воздействий программного средства на объекты вычислительной системы.

Рассмотрим содержание основных показателей и метрик агрессивности программного средства.

Показатель «зараженности» $П_1$: - показатель, характеризующий мощность конечного множества агрессивных программных элементов в программном средстве.

*Критерии оценки :*Уровень агрессивности программного средства прямо зависит от мощности множества АПЭ. Агрессивность по данному показателю будем определять с помощью априорно заданной функции принадлежности множества значений степени «зараженности» программного средства уровню агрессивности программного средства - μ^1 . В простейшем случае функция μ^1 может иметь вид линейной зависимости

*Метрики оценки :*В качестве основы формирования исходных и производных метрик могут быть использованы метрики Холстеда []:

1) N_1 – общее количество программных элементов в программе;
2) N_2 – количество агрессивных программных элементов в ПС.

Производные метрики:

1) $I = N_2 / N_1$ – степень “зараженности” программы. $I \in [0 ; 1]$.
2) $П_1 = \mu^1(I)$. Значение I определяет агрессивность ПС с помощью функции принадлежности μ^1.

Показатель опасности $П_2$: - показатель степени опасности разрушающего программного воздействия программного средства.

Критерии оценки : Уровень агрессивности программного средства также зависит от того, какой тип(ы) разрушающей функции(ий) агрессивных программных элементов обнаружены в нем. Тип разрушающей функции связывается с определенной степенью опасности возможного разрушающего воздействия. Для обнаружения таких воздействий существует ряд практических способов [10,11].

Под степенью опасности будем понимать возможность реализации разрушающей функции АПЭ.

Метрики оценки :

1) $V^* = \{v^*_1, v^*_2, \ldots, v^*_s\}$ – множество обнаруженных типов разрушающих функций исследуемого программного средства;

2) μ^2 (V) – функция принадлежности множества всех типов разрушающих функций v_1, v_2, …, v_n степени их опасности. Степень опасности оценивается для конкретной системы. Вид μ^2 (V) определяется экспертным путем исходя из назначения, архитектуры, обработки информации, защиты вычислительной среды.

3) $П_{2i} = \mu^2 (v^*_i)$ – оценка степени опасности i-го типа разрушающей функции, обнаруженной в программном средстве, i = 1, …, s; - определяется по графику функции принадлежности μ^2 (V);

Таким образом, введенное в рассмотрение новое свойство ПС позволяет прогнозировать его влияние на ход вычислительного процесса.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК ЛИТЕРАТУРЫ

1. Волков Е.И., Осипенко И.А. Анализ вирусной опасности и средства по ее нейтрализации на примере "WANNACRY" // Интеллектуальные ресурсы – региональному развитию. – Ростов-на-Дону, 2019. – Том 5, № 2. – С. 25-31. – URL:https://www.elibrary.ru/item.asp?id=41353618 (дата обращения: 18.01.2020).
2. Храмов В.В. и др. Защита информации в вычислительных системах: Учебное пособие для вузов. – М.,2002. – 192 с. –URL:https://elibrary.ru/item.asp?id=32762286 (дата обращения: 18.01.2020).
3. Алекперов И.Д. и др. Информационная безопасность и защита информации в цифровой экономике. Элементы теории и тестовые задания: Учебное пособие. – Ростов-на-Дону, 2020. – 114 с.
4. Храмов В.В., Трубников А.Н. Модель элементарной защиты программного средства // Информационные технологии и проблемы микроэлектроники: Сборник научных статей / под ред. докт. тех. наук, проф. В.А. Бархоткина. – М., 1999. – С. 192-197. – URL:https://elibrary.ru/item.asp?id=327112590 (дата обращения: 18.01.2020)
5. Храмов В.В.Основы методологии синтеза средств защиты информации // Проблемы обеспечения эффективности и устойчивости функционирования сложных технических систем: Материалы XXI Межведомственной научно-технической конференции. – 2002. – С. 115-120. – URL: https://elibrary.ru/item.asp?id=32877301(дата обращения: 18.01.2020).
6. Храмов В.В., Хадыка А.С.Разработка принципов, методов и средств самоорганизации систем защиты информации // Транспорт-2006: Труды Всероссийской научно-практической конференции. – Ростов-на-Дону, 2006. – С. 230-232. – URL: https://elibrary.ru/item.asp?id=32632220 (дата обращения: 18.01.2020).
7. Голубенко Е.В., Ковтун О.Г. и др. Информационная безопасность и защита информации на транспорте: Тестовые задания по дисциплине. – Ростов-на-Дону, 2015. – URL:https://elibrary.ru/item.asp?id=36311930 (дата обращения: 18.01.2020).
8. Khramov V.V., Trubnikov A.N.Analysis of the aggressiveness of a software product //Automatic Control and Computer Sciences. – 1999. – Т. 33,№2.–С. 28-34. – URL:https://elibrary.ru/item.asp?id=13328155.

9. Губарев О.К. и др. Способ повышения безопасности программных средств и пути его реализации // Тематический научно-технический сборник. – Пущино, 1994. – С. 56-61. – URL: https://elibrary.ru/item.asp?id=32837963.
10. Ковтун О.Г. и др. Способ контроля правильности выполнения алгоритмов бортовым компьютером при дистанционном зондировании земной поверхности // Системные проблемы надёжности, качества, компьютерного моделирования, информационных и электронных технологий в инновационных проектах (ИННОВАТИКА – 2014): Материалы Международной конференции, Российской научной школы и Форума. – 2014. – С. 157-158. – URL:https://elibrary.ru/item.asp?id=36379744 (дата обращения: 18.01.2020).
11. Ковтун О.Г. и др.Терминальный способ контроля исполнения алгоритмов бортовым компьютером на железнодорожном транспорте // Вестник РГУПС. – 2015. – № 1 (57). – С. 61-68. – URL: https://elibrary.ru/item.asp?id=23491949 (дата обращения: 18.01.2020).