УДК 004.9

МОДЕЛИРОВАНИЕ КИБЕРБЕЗОПАСНОСТИ ПРИ ПРИНЯТИИ УПРАВЛЕНЧЕСКИХ РЕШЕНИЙ

Горбачева А.А.

Аспирант третьего года обучения,

ЧОУ ВО ЮУ (ИУБиП),

e-mail: aa_g98@yandex.ru

Аннотация: Рассматриваются вопросы построения и исследования мягких моделей кибербезопасности в условиях цифровизации социально-экономической сферы. Сформулированы условия и порядок построения методики анализа безопасности программных средств, указываются показатели и критерии достаточности программно-аппаратных средств защиты данных с учетом НЕ-факторов реальных систем принятия решений.

Ключевые слова: кибербезопасность, программная закладка, разрушающее программное средство, мягкая модель

MODELING CYBER SECURITY IN ADMINISTRATION OF MANAGEMENT DECISIONS

Gorbacheva A.A.

Graduate student of the third year of study,

PEI HE Southern University (IMBL),

e-mail: lll@yandex.ru

Abstract: The issues of building and researching soft cybersecurity models in the context of digitalization of the socio-economic sphere are considered. The conditions and the procedure for constructing a methodology for analyzing software security are formulated, indicators and criteria for the adequacy of software and hardware data protection are specified, taking into account the non-factors of real decision-making systems.

Keywords: cyber security, software bookmark, destructive software, soft model.

В ходе исследований рассмотрена структура методики анализа безопасности программного средства (ПС), которая включает следующую последовательность шагов:

1. Предварительный анализ условий получения и применения программного средства. Анализ программного средства как объекта защиты.

2. Анализ возможных нарушителей. Формирование моделей

нарушителей. Определение их свойств, демаскирующих признаков, механизмов функционирования, методов маскировки.

3. Определение перечня требований по безопасности, требуемого уровня безопасности. Формирование модели безопасности программного средства.

4. Выбор показателей безопасности ПС. Формирование метрик, расчетных соотношений для определения частных и комплексных показателей безопасности.

5. Оценка частных показателей безопасности программного средства. Нормирование показателей в пределах универсальной единичной шкалы.

6. Проверка попадания значений показателей безопасности ПС в допустимый диапазон изменения. При выходе значений показателей за допустимые границы – уточнение метрик и переход к шагу 4.

7. Определение интегрального показателя уровня безопасности ПС («свертка» частных показателей). Сопоставление значения интегрального показателя нормативному уровню безопасности программного средства.

8. Проверка достоверности оценки уровня безопасности ПС в процессе его эксплуатации в вычислительной системе с реализацией максимального количества угроз безопасности. В случае несоответствия фактического уровня безопасности полученному в результате аттестации: уточнение характеристик нарушителей, определение новых классов нарушителей – переход к шагу 2 или доопределение требований по безопасности к ПС – переход к шагу 3.

9. Проверка соответствия фактического уровня безопасности программного средства требуемому уровню. Выдача научно-обоснованных рекомендаций по приведению к требуемому уровню безопасности.

Процесс оценки уровня безопасности программ представляет собой оценку показателей безопасности и может быть описан следующим алгоритмом:

1. Сбор исходных данных и заполнение информационных таблиц об объекте защиты, каналах утечки информации.

2. Сбор исходных данных и заполнение информационных таблиц о потенциальных нарушителях в вычислительной системе.
3. Ввод данных, характеризующих требования по безопасности.
4. Расчет значений частных показателей безопасности программного средства по заданным метрикам.
5. Нормирование показателей в пределах универсальной единичной шкалы.
6. Определение интегрального показателя безопасности программного средства.

Определена классификация разрушающих программных средств с использованием введенного понятия ПЗ. Под программной закладкой понимается информационный ресурс, «как правило, скрытый в объекте-носителе, являющемся одной из форм представления программы, и реализующий некоторую разрушающую функцию (или совокупность разрушающих функций)»[2].

В существующих классификациях программных закладок (ПЗ) они не рассматриваются как обобщение разрушающих ПС, как, например, вирусов. Устранение этого недостатка достигается [3] обобщенной классификацией программных закладок, предполагающей разделение программных закладок на вирусный и специальный тип.

Тогда функционирующая ПЗ (или программа, содержащая ПЗ) является в ПАС субъектом – S, описывающем преобразование, которому выделен домен (ресурсы системы) и передано управление. При таком определении, «субъект для реализации преобразования использует информацию, содержащуюся в объекте О, т.е. осуществляет доступ к объекту О»[2].

Нелегитимные действия представляют собой композицию следующих операторов [2,4]:

1) $I(O_i,S)$ - оператор настройки ПЗ (исследование ПАС закладкой);
2) $A(O_i,S)$ - оператор доступа к объекту атаки (активизацию ПЗ);
3) $R(O_i)$ - оператор разрушения объекта (разрушающая функция);

4) $M(O_i,S)$ - оператор адаптации (маскировка закладки в ПАС).

Выполнение данных операторов вносит возмущение в программно-аппаратную среду, что отображено использованием в параметрах операторов O_i [5].

В терминах этих операторов нелегитимный процесс в ПАС, инициированный некоторым «чужеродным» субъектом и приводящий к нарушению безопасности и целостности O_i описывается следующим уравнением:

$$V = V ([M (O_k, S)] ([I (O_j, S)] , A (O_i, S), R (O_i))). \quad (2)$$

В общем случае $i \neq j \neq k$. При этом[6] задача анализа субъекта сводится к нахождению у него функций, реализующих данные операторы.

Кроме выявления структуры и особенностей функционирования потенциального нарушителя важным пунктом методики анализа безопасности программного средства является обоснование и выбор показателей безопасности, произведенный в работе на основе мягкой модели безопасности (ММБ) ПС в условиях реализации РПВ.

ММБ ПС применительно к современным условиям ведения информационной войны, представленная на рисунке 1, отображает следующие разрушающие воздействия ПС на ВС:

- программные закладки (атака РПВ);
- выходные данные ПС, нарушающие целостность и безопасность ВС - D_p ($D_p \subseteq F_т$), где $F_т$ – множество функций ПС, заданных техническими требованиями на ее разработку [7];
- несанкционированный (НСД) и нелегитимный (НЛД) доступы;
- ошибки и искажения выходных данных ПС – D.

Таким образом, рассмотрена и проанализирована модель кибербезопасности вычислительных средств типовой компании в условиях неполноты исходных данных. Результаты этого анализа показана ее адекватность реальным условиям.

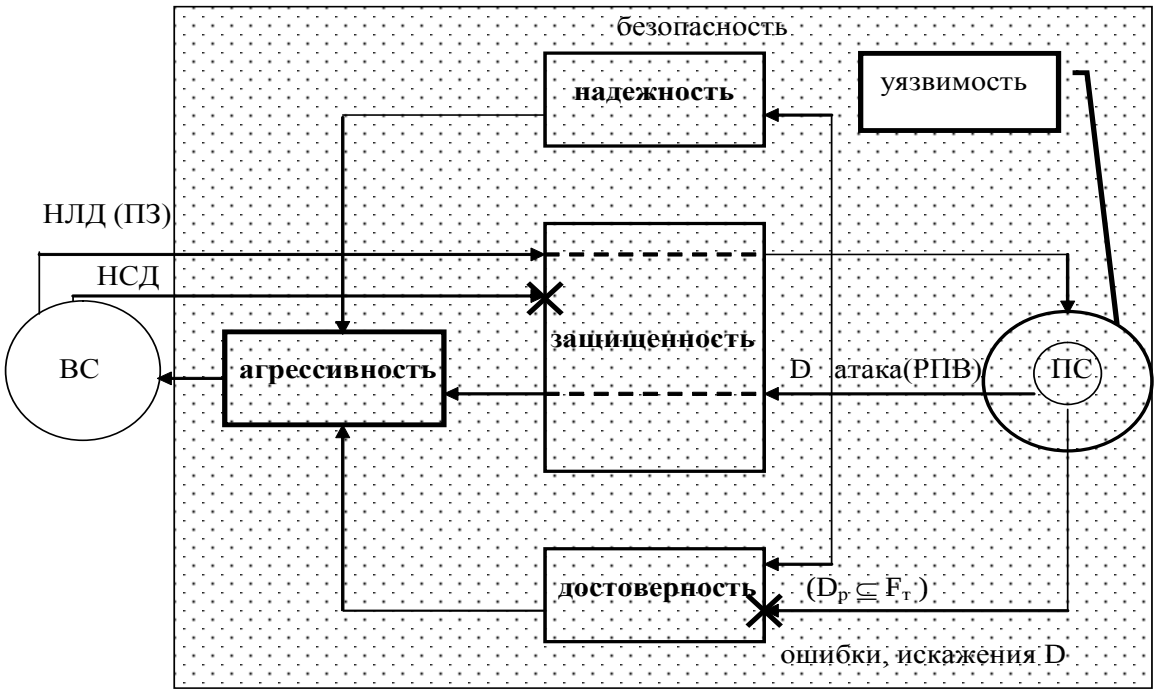

Рис.1 – Модель программного средства

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 02.02.2020).
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 02.02.2020).
3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания: учеб.пособие / И.Д. Алекперов, В.В. Храмов, А.А. Горбачева, Д.П. Фомичев; ЮУ (ИУБиП). – 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.: МИЭТ, 1999. – С. 192-197. URL:https://elibrary.ru/item.asp?id=327112590 (дата обращения 02.02.2020).
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 02.02.2020).
6. 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 02.02.2020).
7. Khramov V.V., Trubnikov A.N.Analysis of the aggressiveness of a software product //Automatic Control and Computer Sciences. – 1999. – Т.33. – С. 28-34. – URL:https://elibrary.ru/item.asp?id=13328155 (датаобращения 02.02.2020).