Методологические основы концепции адаптивного управления защищенностью информационных ресурсов автоматизированных систем специального назначения от вирусных атак

Р.А. Хворов, e-mail: khvoroff@rambler.ru[1]
С.В. Скрыль, e-mail: zi@bmstu.ru [2]

[1] ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» (г. Воронеж)
[2] МГТУ имени Н.Э. Баумана

Аннотация. *В статье рассмотрены теоретические основы адаптивного управления защитой информации объектов информационной инфраструктуры автоматизированных системах специального назначения.*

Ключевые слова: *Управление защищенностью, адаптивное управление, информационные ресурсы.*

Введение

Для понимания и трактовки адаптивного управления защищенностью информационных ресурсов автоматизированных систем специального назначения (АС СН) от вирусных атак как исследуемого явления сформируем концепцию построения соответствующей исследовательской среды.

Изучение такого явления как адаптивное управление защищенностью информационных ресурсов АС СН от вирусных атак, обусловлено наличием двух взаимосвязанных объектов исследования – угроз вирусных атак на информационные ресурсы и применяемых в рассматриваемой информационной инфраструктуре механизмов управления состояниями ее защищенности. Исходя из этого в качестве методологической основы данной концепции следует рассматривать теорию управление [1] и теорию информационной безопасности [2], а в качестве методической основы – закономерности практики обнаружения, предупреждения и ликвидации последствий вирусных атак [3].

Концепция адаптивного управления защищенностью информационных ресурсов АС СН от вирусных атак

Концепция адаптивного управления защищенностью информационных ресурсов АС СН от вирусных атак, как и любая концепция, представляется теоретическими и прикладными основаниями. Теоретические основания позволяют сформулировать ряд методологических положений относительно реализации управления защищенностью объектов рассматриваемого типа исходя из возможности адекватной оценки текущего и прогнозируемого ее состояний, а также методологических положений относительно возможности системного представления характеристик защищенности. Прикладные основания рассматриваемой концепции обусловливают возможность реализации принципов адаптивного управления процессами обнаружения, предупреждения и ликвидации последствий вирусных атак на информационные ресурсы информационных ресурсов АС СН.

Основополагающими принципами, на которых базируется концепция являются принципы дифференциации исследуемого явления и интегрированности применяемого методологического аппарата. Принцип дифференциации в концепции адаптивного управления защищенностью информационных ресурсов АС СН от вирусных атак предполагает структуризацию целевых функций исследуемых объектов – целевой функции вирусных атак и целевой функции процессов обнаружения, предупреждения и ликвидации их последствий. В соответствии со вторым принципом имеет место интегральное представление показателя защищенности информационных ресурсов АС СН от вирусных атак как управляемой характеристики.

Содержание концепции адаптивного управления защищенностью информационных ресурсов АС СН от вирусных атак логически вытекает из содержания понятий «управляемость», «адаптация», «эффективность» и «защищенность».

В общем случае управляемость трактуется как «возможность целенаправленного перевода (перехода) системы посредством управления из одного состояния в другое – требуемое» [4]. В случае адаптивного управления защищенностью информационных ресурсов АС СН от вирусных атак под управляемостью будем понимать способность механизмов управления защищенностью осуществлять перераспределение используемых в АС СН временных ресурсов с целью обеспечения ее уровня выше требуемого.

С целью анализа содержания адаптивного управления защищенностью информационных ресурсов АС СН от вирусных атак

рассмотрим понятия адаптации. Согласно [5] адаптация это «(лат. adapto – приспособляю) – процесс приспособления системы к условиям внешней и внутренней среды».

В случае данного исследования под адаптацией будем понимать периодическую оценку состояния защищенности информационных ресурсов АС СН от вирусных атак с последующей функциональной реструктуризацией механизма антивирусной защиты с целью обеспечения уровня защищенности выше требуемого.

В общеметодологическом (философском) плане понятие «эффективность» (лат. efficientia) трактуется, как способность действующей причины произвести определённый эффект [6]. В случае данного исследования эффект будет состоять в обеспечении конфиденциальности, целостности и доступности информации.

Исходя из этого под «защищенностью» информационных ресурсов АС СН от вирусных атак, будем понимать способность механизмов обнаружения, предупреждения и ликвидации последствий такого рода угроз обеспечивать эффект восприятия нарушения безопасности информации, как одного из допустимых состояний используемой информационной технологии, обрабатываемого данными механизмами. Отсюда становится очевидным, что понятие «защищенность» информационных ресурсов АС СН от вирусных атак характеризует совокупность свойств механизмов обнаружения, предупреждения и ликвидации последствий такого рода угроз, обусловливающих способность такого рода механизмов к реализации своей целевой функции – обеспечению значений характеристик конфиденциальности, целостности и доступности информации не ниже требуемого уровня. Кроме того, исходя из данного определения, предполагается наличие двух групп функциональных характеристик – характеристик угроз вирусных атак на информационные ресурсы информационных ресурсов АС СН и характеристик процессов обнаружения, предупреждения и ликвидации последствий такого рода угроз.

Заключение

Таким образом, с учетом выше изложенного следует определить ряд общих положений, позволяющих сформировать структуру концепции адаптивного управления защищенностью информационных ресурсов АС СН от вирусных атак. К таким положениям относятся следующие:

1. Разработка концептуальных решений по принципам адаптации процесса управления защищенностью информационных ресурсов АС СН от вирусных атак к уровню такого рода угроз.

2. Характеристика возможностей нарушителя по реализации вирусных атак на информационные ресурсы информационной инфраструктуры АС СН и возможностей механизмов обнаружения, предупреждения и ликвидации последствий такого рода угроз, как факторов, оказывающих влияние на их защищённость.

3. Формирование структурного представления процессов обнаружения, предупреждения и ликвидации последствий вирусных атак, как следствия такого рода угроз.

4. Обоснование системной классификации характеристик мер обеспечения защищенности информационных ресурсов АС СН от вирусных атак на основе анализа различных вариантов реализации такого рода угроз и процессов их обнаружения, предупреждения и ликвидации последствий.

5. Формирование структуры методологического аппарата для исследования вирусных атак на информационные ресурсы АС СН и процессов обнаружения, предупреждения и ликвидации последствий такого рода угроз.

6. Выбор математических абстракций для формализованного представления исследуемых процессов, разработка соответствующих математических моделей.

7. Структурирование исследовательской среды для моделирования вирусных атак на информационные ресурсы АС СН и процессов обнаружения, предупреждения и ликвидации последствий такого рода угроз с целью оценки характеристик исследуемых процессов.

8. Выбор инструментальных средств для идентификация состояний защищенности информационных ресурсов АС СН

9. Формирование условий, обеспечивающих реализацию адаптивного управления механизмами обнаружения, предупреждения и ликвидации последствий вирусных атак.

Список литературы

1. Земедлина Е.А. Теория управления. – М.: Риор, 2017. – 752 с.

2. Информационная безопасность систем организационного управления. Теоретические основы. Том 1. – М.: Наука, 2016. – 496 с.

3. Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

4. Кибернетика конструктивная. Словарь терминов. (Электронный ресурс)

5. Ильичев Ф., Федосеев П.Н. Философский энциклопедический словарь. – М.: Сов. Энциклопедия, 1983. – 840 с.

6. Философский словарь: Сост. И.Т Фролов. – М.: Политиздат, 1991. – 470 с.