Е. Б. Дроботун

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

Е. Б. Дроботун

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ОТ КОМПЬЮТЕРНЫХ АТАК ДЛЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

МОНОГРАФИЯ

Санкт-Петербург
Наукоемкие технологии
2017

УДК 004.056.52(57)
ББК 32.973.2-018
Д75

Рецензенты:

Главный научный сотрудник управления ФАУ «Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России», доктор технических наук, профессор **Язов Юрий Константинович**

Доцент кафедры систем и сетей связи космических комплексов Военно-космической академии им. А. Ф. Можайского, кандидат технических наук, доцент **Макаренко Сергей Иванович**

Дроботун Е. Б.

Д75 Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. – СПб.: Наукоемкие технологии, 2017. – 120 с., ил.

ISBN 978-5-9909412-2-9

В монографии предложены теоретико-методологические подходы к решению задачи формирования перечня актуальных для защищаемой автоматизированной системы компьютерных атак, задачи формирования функциональных требований к системе защиты, а также теоретико-методологический подход к решению задачи построения системы защиты от компьютерных атак.

Монография предназначена для научных работников и специалистов в области проектирования систем защиты от компьютерных атак для автоматизированных систем управления различного назначения.

УДК 004.056.52(57)
ББК 32.973.2-018

ISBN 978-5-9909412-2-9

© Дроботун Е. Б., 2017
© Наукоемкие технологии, 2017

Научное издание.
Напечатано с оригинал-макета, подготовленного автором.

Оглавление

Введение 5

1 Основные положения теории защиты автоматизированных систем от компьютерных атак 8

1.1 Современное состояние вопросов построения систем защиты от компьютерных атак для автоматизированных систем управления 8

1.2 Определения и основные понятия 14

1.3 Модели защиты от компьютерных атак 33

1.3.1 Модель защиты от компьютерных атак на основе нормативно-гарантированного подхода 37

1.3.2 Модель защиты от компьютерных атак на основе риск-ориентированного подхода 39

1.4 Стратегии защиты от компьютерных атак 41

1.5 Постановка задачи выбора оптимального варианта построения системы защиты от компьютерных атак 45

2 Теоретико-методологический подход к формированию функциональных требований к системе защиты от компьютерных атак 52

2.1 Общая концепция формирования функциональных требований к системе защиты от компьютерных атак с использованием риск-ориентированного подхода 52

2.2 Исходные теоретические положения по формированию функциональных требований к системе защиты от компьютерных атак 53

2.3 Оценка количественных характеристик рисков нарушения безопасности автоматизированной системы управления при воздействии компьютерных атак 58

2.4 Формирование функциональных требований к системе защиты от компьютерных атак 62

3 Теоретико-методологический подход к выбору оптимального варианта построения системы защиты от компьютерных атак 71

3.1 Общая концепция выбора оптимального варианта построения системы защиты от компьютерных атак 71

3.2 Сущность и содержание этапов выбора оптимального варианта построения системы защиты от компьютерных атак .72

3.2.1 Формирование множества альтернативных вариантов построения системы защиты от компьютерных атак 72

3.2.2 Формирование допустимых по стоимости вариантов построения системы защиты от компьютерных атак 79

3.2.3 Формирование предпочтительных вариантов построения системы защиты от компьютерных атак 81

3.2.4 Выбор оптимального варианта построения системы защиты от компьютерных атак 88

Заключение.....93

Литература 94

Приложение А.....110

Приложение Б 113

Приложение В.....115

Приложение Г 117

Приложение Д.....118

Введение

Создание автоматизированных систем управления, устойчивых к различным информационно-техническим воздействиям (в том числе и к компьютерным атакам) сопряжено с существенными затратами как времени, так и материальных ресурсов. Также необходимо отметить, что введение в состав автоматизированных систем управления каких-либо средств защиты от компьютерных атак влечет за собой снижение качества функционирования защищаемой системы вследствие того, что введенные в состав защищаемой системы средства защиты требуют определенных вычислительных ресурсов, количество которых в защищаемой системе конечно и ограниченно. Помимо этого, существует известная обратная зависимость между удобством пользования системой и её защищённостью: чем совершеннее системы защиты, тем сложнее пользоваться основным функционалом информационной системы.

Исходя из вышесказанного, задача построения оптимальной (с точки зрения потребляемых вычислительных ресурсов) системы защиты от компьютерных атак для автоматизированных систем управления различного назначения представляется весьма актуальной.

Задача построения оптимальной системы защиты автоматизированных систем управления от компьютерных атак является достаточно сложной и многогранной. Она включает в себя как теоретические и методологические аспекты, так и практические, связанные с разработкой, проектированием и построением как отдельных средств защиты от компьютерных атак, так и многокомпонентных систем защиты.

Целью данной работы является разработка теоретико-методологических подходов, позволяющих теоретически обосновать функциональные требования к системам защиты от компьютерных атак, а также провести выбор оптимального (с точки зрения потребляемых ресурсов защищаемой автоматизированной системы) варианта построения системы защиты от компьютерных атак для автоматизированных систем управления.

Под оптимальным вариантом построения системы защиты от компьютерных атак далее будет пониматься такая совокупность

отдельных средств защиты, обладающих определенными функциональными возможностями, которая будет обеспечивать требуемую эффективность защиты от компьютерных атак и, в то же время, будет потреблять минимальное количество ресурсов защищаемой системы.

Монография включает в себя три главы, в которых изложены теоретические положения, касающиеся проблематики построения систем защиты от компьютерных атак и, на основе этих положений, предложен теоретико-методологический подход, позволяющий обосновать и сформировать систему защиты от компьютерных атак с оптимальной структурой.

В первой главе анализируется современное состояние вопросов защиты информационно-вычислительных (автоматизированных) систем различного назначения от компьютерных атак, излагаются методологические основы защиты информации в информационно-вычислительных (автоматизированных) системах и обеспечения их безопасного функционирования в условиях различных информационно-технических воздействий (в том числе и в условиях компьютерных атак), уточнен и определен понятийный аппарат, а также показано, что выбор оптимального варианта построения системы защиты от компьютерных атак является сложной многокритериальной задачей принятия решения.

Во второй главе изложен теоретико-методологический подход к решению задачи формирования перечня актуальных для защищаемой автоматизированной системы управления компьютерных атак, а также задачи формирования функциональных требований к системе защиты.

Третья глава посвящена изложению теоретико-методологического подхода к решению задачи выбора оптимального варианта построения системы защиты от компьютерных атак.

Предложенный в третьей главе подход основан на поэтапном формировании множества альтернативных вариантов построения системы защиты от компьютерных атак и множества предпочтительных вариантов построения системы защиты с последующим выбором оптимального варианта построения системы защиты из множества предпочтительных вариантов построения системы защиты.

Автор выражает признательность рецензентам рукописи монографии – доктору технических наук, профессору Язову Юрию Константиновичу и кандидату технических наук, доценту Макаренко Сергею Ивановичу.

1 Основные положения теории защиты автоматизированных систем от компьютерных атак

1.1 Современное состояние вопросов построения систем защиты от компьютерных атак для автоматизированных систем управления

Проведенный анализ работ и результатов исследований, предпринятых различными авторами, показывает, что современное состояние разработки вопросов обеспечения защищенности автоматизированных систем от информационно-технических воздействий (в том числе и от компьютерных атак), а также построения систем защиты от компьютерных атак располагает достаточно большой теоретико-методологической и практической базой для исследования и решения проблем построения систем защиты от компьютерных атак для автоматизированных систем управления различного назначения, а большинство научных работ и исследований представлены четырьмя группами.

Первая группа представлена работами, в которых исследуются и предлагаются различные способы защиты информационно-вычислительных и автоматизированных систем от информационно технических воздействий (в том числе и от компьютерных атак), в виде отдельных технических или технологических решений.

Данная группа объединяет таких авторов как: Д. Ю. Гамаюнов [22], Ю. В. Бородакий [17, 100, 102], С. Н. Гриняев [37, 39], В. М. Зима, А. А. Молдавян, Н. А Молдавян [63], М. А. Иванов [65], И. В. Котенко [80], С. М. Климов, М. П. Сычев, А. В. Астрахов [74], Е. В. Гречишников [101, 103], И. Б. Саенко [80, 125, 126] и др.

В этих работах представлены исследования, которые позволили расширить перечень и увеличить число способов защиты информационно-вычислительных и автоматизированных систем от отдельных видов информационно-технических воздействий.

Вторая группа представлена работами, в которых анализируются возможные способы информационно-технических воздействий, исследуются и предлагаются способы моделирования, оценки и обеспечения защищенности информационно-вычислительных и автоматизированных систем от различных

информационно-технических воздействий, а также предлагаются подходы к выработке и обоснованию требований по обеспечению защищенности информационно-вычислительных и автоматизированных систем от различных информационно-технических воздействий (в том числе и от компьютерных атак).

Данная группа объединяет таких авторов как: С. Н. Гриняев [38], В. И. Емелин [55], А. А. Бойко [15], С. А. Будников, В. П. Жуматий, Н. В. Паршин [57], М. А. Коцыняк, И. А. Кулешов, А. М. Кудрявцев, О. С. Лаута [71], Ю. Л. Козирацкий [76, 77], А. Г. Корченко [79], С. И. Макаренко [86], Г. А. Остапенко [66, 99], П. И. Тутубалин, В. С. Моисеев, К. В. Иванов [64, 136], Ю. К. Язов [142, 143] и др.

В работах авторов указанной группы исследуются отдельные частные вопросы теории информационной безопасности, такие как:

– анализ, моделирование и оценка рисков в информационных (автоматизированных) системах [66, 76, 77, 79, 99];

– анализ и моделирование информационно-технических воздействий (в том числе и компьютерных атак) и компонентов систем защиты [15, 38, 57, 64, 66, 71, 86, 99, 92, 136, 143];

– разработка методик оценки эффективности систем защиты от компьютерных атак, а также отдельных элементов таких систем [64, 79, 136, 142, 143];

– разработка методик выработки требований к системам защиты от информационно-технических воздействий [64, 71, 136, 143];

– исследование вопросов устойчивости функционирования информационных (автоматизированных) систем различного назначения в условиях информационно-технических воздействий (в том числе и компьютерных атак) [55, 57, 64, 71].

Третья группа представлена работами, в которых исследуются и предлагаются методы, модели и методики проектирования и построения систем защиты информационно-вычислительных и автоматизированных систем от различных видов информационно-технических воздействий, а также методы обеспечения безопасного функционирования автоматизированных систем управления.

Данная группа объединяет таких авторов как: Р. М. Алгулиев [2], Ю. В. Бородакий [16], С. А. Будников, Н. В. Паршин [18], А. Н. Буренин, К. Е. Легков [19], О. Ю. Гаценко [23], В. Е. Дементьев, Ю. И. Стародубцев, М. А. Коцыняк [43],

В. В. Домарев [44], И. В. Котенко [59], Д. П. Зегжда [61], О. В. Казарин [67], С. М. Климов [72], В. В. Липаев [82], О. В. Лукинова [84], С. Н. Новиков [94], В. Г. Кулаков, В. Г. Кобящев [96], В. В. Зима, А. Г. Ломако, М. М. Котухов, А. С. Марков, А. А. Молдавян [111], Е. А. Рогозин [114], А. Ю. Щербаков [140] и др.

В указанных работах исследуются различные комплексные подходы (в том числе законодательные, организационные и организационно-технические) к построению систем защиты автоматизированных систем от информационно-технических воздействий.

Из этой группы следует выделить работы В. В. Домарева [44], О. В. Казарина [67], С. М. Климова [72], В. В. Липаева [82], С. Н. Новикова [94], а также работу [111].

В работе [44] изложены причины нарушения безопасности компьютерных систем, приведено описание математических моделей систем защиты информации, а также рассмотрены методы и средства внедрения механизмов защиты в существующие информационные системы с возможностью гибкого управления безопасностью в зависимости от выдвигаемых требований, допустимого риска и оптимального расхода ресурсов.

В монографии [67] рассмотрены теоретические и прикладные аспекты проблемы обеспечения безопасности программного обеспечения компьютерных систем различного назначения. Особое внимание уделено моделям и методам создания высокозащищенных и алгоритмически безопасных программ для применения в системах критических приложений.

Работа [72] посвящена вопросам обеспечения устойчивости функционирования критически важных информационных сегментов в условиях воздействия компьютерных атак. В указанной работе предложены и обоснованы технологии противодействия компьютерным атакам, определены принципы классификации компьютерных атак и на их основе произведена наиболее полная классификация компьютерных атак.

В монографии [82] рассмотрены основные факторы, определяющие надежность и безопасность функционирования программных комплексов, на основе которых строятся автоматизированные системы управления. Определены требования к проектированию функциональной пригодности сложных

программ, организация, планирование и процессы разработки требований к безопасности программных продуктов.

Работа [94] посвящена созданию методологических основ, применения технологий сетевого уровня (протоколов маршрутизации и сигнализации) мультисервисных сетей связи для защиты информации.

В работе [111] описывается комплексный подход к решению проблемы информационно-компьютерной безопасности, основанной на учете всех возможных факторов и обеспечивающий достижение требуемого уровня защищенности информации и процесса ее обработки. Раскрываются уязвимости компьютерных сетей и систематизируются способы несанкционированного доступа к электронной информации. Рассматриваются наиболее важные требования к современной системе информационно-компьютерной безопасности и описываются базовые этапы ее построения.

Четвертая группа включает в себя работы, в которых рассматриваются научно-теоретические положения, позволяющие обосновать пути построения систем защиты от информационно-технических воздействий и пути построения систем защиты информации от несанкционированного доступа.

Данная группа объединяет таких авторов как: Г. А. Остапенко, В. И. Белоножкин [13], В. А. Герасименко, А. А. Малюк [24, 25], А. А. Грушо, Е. Е. Тимонина [41], П. Н. Девянин [42], Д. П. Зегжда, А. М. Ивашко [60], А. Г. Мамиконов, В. В. Кульба, А. Б. Шелков [89], С. А. Петренко, Д. Д. Ступин [109], А. П. Росенко [115], П. Д. Зегжда [127] и др.

Работа [13] посвящена теоретическим аспектам и развитию научно-методических основ обеспечения безопасности социотехнических систем в плане моделирования террористических операций и атак на информационные пространства сферы государственного и муниципального управления.

В работе [24] с позиций системно-концептуального подхода рассмотрен широкий круг вопросов, относящихся к защите информации, накапливаемой, хранимой и обрабатываемой в современных автоматизированных системах и сетях. В этой работе описывается методология анализа и синтеза систем обеспечения

безопасности информации, исходя из комплексного взаимодействия ее компонентов, рассматриваемых как система.

Работа [25] посвящена фундаментальным основам защиты информации в автоматизированных системах. В ней рассматриваются общеметодологические принципы разработки теории защиты информации; описываются стратегии и концепции защиты информации в автоматизированных системах; определяются угрозы и методология оценки уязвимости информации; предлагаются методы определения требований к защите информации в автоматизированных системах управления.

Работа [41] посвящена введению в формальную теорию защиты информации. В указанной работе определены и обоснованы теоретические положения доказательного подхода к построению систем защиты и определению политик безопасности. В этой работе предлагается гарантированную защищенность автоматизированной системы понимать как гарантированное выполнение заданных политик безопасности.

В работе [42] рассмотрены с полным доказательством положения основных моделей безопасности информационно-вычислительных систем: дискреционного, мандатного и ролевого разграничения доступа; безопасности информационных потоков, а также изолированной программной среды.

В работе [60] описываются основные положения базовых стандартов, посвященных безопасности информационных технологий; исследуются нарушения безопасности информации в информационно-вычислительных системах; рассматриваются формальные модели безопасности и принципы их использования при построении систем защиты, а также анализируются существующие архитектуры защищенных систем.

В монографии [89] рассмотрены формализованные модели и методы анализа и синтеза механизмов контроля и обеспечения достоверности обрабатываемых данных, требуемого уровня их защиты от несанкционированного доступа и необходимого уровня резервирования, а также проведен анализ путей повышения эффективности отладочных работ как средства уменьшения ошибок в программах и данных. В указанной работе введены понятия механизмов контроля и защиты информации, стандартной схемы обработки информации, индикаторного графа и ошибок.

Данные понятия позволяют осуществлять формальный анализ потоков данных с точки зрения их достоверности и доступности.

В монографии [109] рассмотрены возможные решения научно-технической проблемы раннего предупреждения о компьютерном нападении на критически важные информационные ресурсы Российской Федерации. Полученные результаты позволили спроектировать открытый сегмент Национальной системы раннего предупреждения о компьютерном нападении.

В монографии [115] представлены методологические подходы к анализу и оценке безопасности конфиденциальной информации с учетом воздействия на нее внутренних угроз. В данной работе предложены математические модели для исследования влияния внутренних угроз на безопасность конфиденциальной информации на основе марковских случайных процессов с дискретными состояниями, имитационного моделирования, теории игр.

В работе [127] предпринята одна из первых попыток отечественных авторов изложить проблемы безопасности компьютерных систем в части касающейся их защиты от вредоносных программных средств. В работе определены основные понятия, связанные с концепцией безопасности, приведены классификация и примеры нарушения безопасности компьютерных систем. Представленные в работе модель вычислительной системы и формальная постановка задачи анализа безопасности программного обеспечения позволили предложить два формальных способа решения задачи обеспечения безопасности компьютерных систем: в пространстве программ (логико-аналитические методы) и в пространстве отношений (контрольно-испытательные методы).

Таким образом, имеющиеся в настоящее время работы могут служить основой для дальнейшего совершенствования теории и практики построения систем защиты от компьютерных атак для автоматизированных систем управления. В частности, для формирования понятийно-терминологического аппарата; научно-методического базиса и системы инструментально-технических средств, позволяющих адекватно описывать процессы защиты в условиях значительной неопределенности и непредсказуемости проявления различных дестабилизирующих факторов (в том числе и компьютерных атак), а также разработки комплекса рабочих моделей, необходимых для решения всех задач защиты от компьютерных атак и обоснования подходов к построению систем

защиты от компьютерных атак и оптимизации их структуры и параметров.

1.2 Определения и основные понятия

В общем, понятие автоматизированной системы определено в [29] как системы, состоящей из персонала и комплекса средств автоматизации его деятельности, реализующей информационную технологию выполнения установленных функций.

Автоматизированные системы управления, как правило, предназначены для формирования воздействий (в виде команд, сигналов и др.) с целью управления некоторыми объектами на основе анализа происходящих в них процессов и поведения [143].

Таким образом, для автоматизированных систем управления (АСУ) основными функциями являются:

– управление объектами (исполнительными механизмами, системами вооружения и т. п.) и (или) процессами (производственными, технологическими и т. п.);

– прием, обработка, хранение и выдача информации.

Автоматизированные системы управления в зависимости от вида управляемого объекта могут делиться на автоматизированные системы управления технологическими процессами, автоматизированные системы управления предприятиями, автоматизированы системы управления воздушным движением, автоматизированные системы управления оружием и военными объектами и т. д [29].

Далее, в работе, под автоматизированной системой управления будет пониматься автоматизированная система управления технологическими процессами.

В качестве объекта управления в таких системах выступает совокупность технологического оборудования и реализованного на нем по соответствующим инструкциям или регламентам технологического процесса.

При этом в отношении объекта управления АСУ комбинируют одновременно выполнение двух важнейших подпроцессов: контроля (измерения) состояния объекта и обратного воздействия (управления) на объект для удержания его в установленных рамках, т. е. процесс управления представляет собой последовательность действий, направленных на контроль и регулирование

последовательности изменений состояния управляемого объекта в соответствии с требуемыми правилами и алгоритмами (рисунок 1.1).

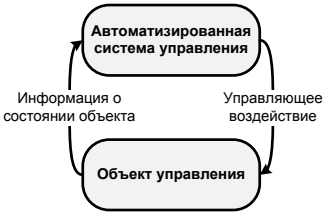


Рисунок 1.1 – Взаимодействие автоматизированной системы управления с объектом управления

Автоматизированная система управления, как правило, имеет многоуровневую структуру (рисунок 1.2) и включает в себя [130, 137]:

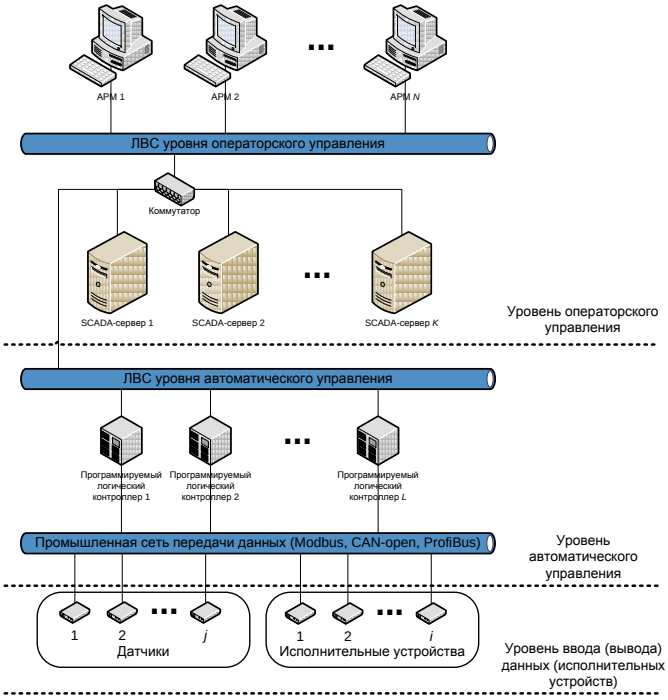


Рисунок 1.2 – Уровни построения автоматизированной системы управления

– уровень операторского (диспетчерского) управления (верхний уровень);

– уровень автоматического управления (средний уровень);

– уровень ввода (вывода) данных, исполнительных устройств (нижний (полевой) уровень).

Автоматизированная система управления технологическими процессами может включать в себя [130]:

а) на уровне операторского (диспетчерского) управления:

операторские (диспетчерские), инженерные автоматизированные рабочие места, промышленные серверы (SCADA-серверы) с установленным на них общесистемным и прикладным программным обеспечением, телекоммуникационное оборудование (коммутаторы, маршрутизаторы, межсетевые экраны, иное оборудование), а также каналы связи;

б) на уровне автоматического управления:

программируемые логические контроллеры, иные технические средства с установленным программным обеспечением, получающие данные с нижнего (полевого) уровня, передающие данные на верхний уровень для принятия решения по управлению объектом и (или) процессом и формирующие управляющие команды (управляющую (командную) информацию) для исполнительных устройств, а также промышленная сеть передачи данных;

в) на уровне ввода (вывода) данных (исполнительных устройств):

датчики, исполнительные механизмы, иные аппаратные устройства с установленными в них микропрограммами и машинными контролерами.

Количество уровней автоматизированной системы управления и ее состав на каждом из уровней зависит от назначения автоматизированной системы управления и выполняемых ею целевых функций. На каждом уровне автоматизированной системы управления по функциональным или иным признакам могут выделяться дополнительные сегменты [130].

В автоматизированной системе управления объектами зашиты являются [130]:

– информация (данные) о параметрах (состоянии) управляемого (контролируемого) объекта или процесса (входная (выходная) информация, управляющая (командная) информация,

контрольно-измерительная информация, иная технологическая информация;

– программно-технический комплекс, включающий технические средства (в том числе автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, каналы связи, программируемые логические контроллеры, исполнительные устройства), программное обеспечение (в том числе микропрограммное, общесистемное, прикладное), а также средства защиты.

Комплекс средств автоматизации, входящий в состав автоматизированной системы управления, в свою очередь может быть определен как множество взаимодействующих программных и программно-аппаратных компонентов автоматизированной системы, а также информационных ресурсов, необходимых для функционирования автоматизированной системы.

Таким образом, АСУ можно представить в виде множества взаимодействующих объектов (компонентов программно-аппаратных и программных средств, информационных ресурсов, а также лиц оперативного и обслуживающего персонала).

Указанные объекты можно разделить на два подмножества:

– подмножество активных объектов АСУ;
– подмножество пассивных объектов АСУ.

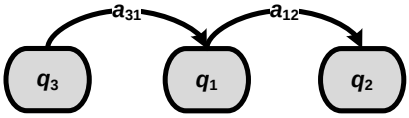


Рисунок 1.3 – Пример взаимодействия активных и пассивных объектов (a_{31} – операция, которую объект q_3 может осуществлять в отношении объекта q_1; a_{12} – операция, которую объект q_1 может осуществлять в отношении объекта q_2)

Пассивный объект не может осуществлять какие-либо операции с другими объектами, тогда как активный – может. При этом, под операциями над объектами понимаются следующие элементарные операции: чтение (rd), уничтожение (del), запуск на выполнение (ex), модификация (перезапись объекта, запись в конец объекта) (mod), создание нового объекта (cr). Необходимо также отметить, что некоторые объекты могут быть одновременно как активными, так и пассивными, т. е., например, объект q_1, который

является активным по отношению к объекту q_2, может быть пассивным в отношении к объекту q_3 (рисунок 1.3)

В дальнейшем будем считать, что *j*-й активный объект, на момент времени t, в отношении *i*-го объекта может совершать только одну операцию.

Определение 1.1. Под автоматизированной системой управления будем понимать множество взаимодействующих объектов:

$$Q = A \cup S \cup C \cup H, \tag{1.1}$$

где A – подмножество аппаратных компонентов АСУ; S – подмножество компонентов программного обеспечения АСУ; C – подмножество информационных ресурсов, хранящихся и (или) обрабатываемых в АСУ; H – подмножество лиц оперативного и обслуживающего АСУ персонала. При этом:

$$Q = Q_{\text{акт}} \cup Q_{\text{пасс}}, \tag{1.2}$$

где $Q_{\text{акт}}$ – подмножество активных объектов АСУ; $Q_{\text{пасс}}$ – подмножество пассивных объектов АСУ.

Для любого (*i*-го) пассивного объекта $q_{\text{пасс}_i} \in Q_{\text{пасс}}$ может быть определено множество $Q_{\text{акт}_i}$ активных объектов, которым разрешено совершать операции над *i*-м пассивным объектом. При этом:

$$Q_{\text{акт}} = Q_{\text{акт}_1} \cup Q_{\text{акт}_2} \cup \ldots \cup Q_{\text{акт}_I}, \tag{1.3}$$

где I – число пассивных объектов; $i = \overline{1;I}$.

В свою очередь, для каждого активного объекта $q_{\text{акт}_{ki}} \in Q_{\text{акт}_i}$ может быть определено множество O_{ki} разрешенных операций, которые активный объект $q_{\text{акт}_{ki}}$ может совершать над пассивным объектом $q_{\text{пасс}_i}$. Это множество можно представить в виде декартового произведения множества $O_{\text{полн}}$ всех возможных операций над пассивным объектом и множества $M_{\text{разр}_{ki}}$ разрешений на проведение операций *k*-м активным объектом над *i*-м пассивным:

$$O_{ki} = O_{\text{полн}} \times M_{\text{разр}_{ki}},\ i = \overline{1;I},\ k = \overline{1;K}, \quad (1.4)$$

где K – число активных объектов, множество $O_{\text{полн}}$ определено следующим образом:

$$O_{\text{полн}} = \{rd; del; ex; mod; cr\}, \quad (1.5)$$

а множество $M_{\text{разр}_{ki}}$:

$$M_{\text{разр}_{ki}} = \left\{m_{rd_{ki}}; m_{del_{ki}}; m_{ex_{ki}}; m_{mod_{ki}}; m_{cr_{ki}}\right\}. \quad (1.6)$$

Элементы множества $M_{\text{разр}_{ki}}$ могут рассматриваться как булевы переменные, которые определяются следующими правилами:

$$m_{rd_{ki}} = \begin{cases} 1, \text{если } k\text{-й активный объект имеет право производить} \\ \text{чтение } i\text{-го пассивного объекта} \\ 0, \text{в противном случае} \end{cases}, \quad (1.7)$$

$$m_{del_{ki}} = \begin{cases} 1, \text{если } k\text{-й активный объект имеет право производить} \\ \text{уничтожение } i\text{-го пассивного объекта} \\ 0, \text{в противном случае} \end{cases}, \quad (1.8)$$

$$m_{ex_{ki}} = \begin{cases} 1, \text{если } k\text{-й активный объект имеет право производить} \\ \text{запуск } i\text{-го пассивного объекта на исполнение} \\ 0, \text{в противном случае} \end{cases}, \quad (1.9)$$

$$m_{mod_{ki}} = \begin{cases} 1, \text{если } k\text{-й активный объект имеет право} \\ \text{производить модификацию } i\text{-го пассивного объекта} \\ 0, \text{в противном случае} \end{cases}, \quad (1.10)$$

$$m_{cr_{ki}} = \begin{cases} 1, \text{если } k\text{-й активный объект имеет право} \\ \text{создавать экземпляр } i\text{-го пассивного объекта} \\ 0, \text{в противном случае} \end{cases}. \quad (1.11)$$

При этом, как и ранее, I – число пассивных объектов; K – число активных объектов.

Помимо этого, для каждого (i-го) пассивного объекта может быть определена переменная $n_{\text{оп}_i}$, которая характеризуют загрузку этого i-го объекта. Значение данной переменной равно числу

одновременно совершаемых операций в отношении i-го пассивного объекта.

Определение 1.2. Состоянием i-го пассивного объекта в момент времени t будем называть пару вида:

$$St_i(t) = (\hat{Q}_{\text{акт}_i}(t), \hat{O}_i(t)), \tag{1.12}$$

где $\hat{Q}_{\text{акт}_i}(t)$ – множество активных элементов, совершаемых операции над i-м пассивным объектом в момент времени t; $\hat{O}_i(t)$ – множество операций, совершаемых активными объектами над i-м пассивным объектом в момент времени t:

$$\hat{O}_i(t) = \{o_{1i}^{(t)}; o_{2i}^{(t)}; \dots; o_{n_{\text{оп}_i}i}^{(t)}\}, \tag{1.13}$$

где $n_{\text{оп}_i}$ определяется как число элементов (мощность) множества $\hat{Q}_{\text{акт}_i}(t)$:

$$n_{\text{оп}_i} = \left|\hat{Q}_{\text{акт}_i}(t)\right|. \tag{1.14}$$

Определение 1.3. Состоянием автоматизированной системы управления в момент времени t будем называть совокупность состояний всех пассивных объектов этой АСУ в момент времени t:

$$St(t) = \{St_1(t); St_2(t); \dots; St_I(t)\}. \tag{1.15}$$

Исходя из этого, функционирование АСУ можно представить в виде некоторой последовательность ее состояний, такой, что каждое последующее состояние (в момент времени $t + \Delta t$) отличается от предыдущего (в момент времени t) состоянием хотя бы одного объекта.

Определение 1.4. Множество состояний АСУ есть непустое конечное множество состояний АСУ, в котором любые два соседних состояния отличны друг от друга:

$$St = \left\{St\big(t + (j \cdot \Delta t)\big)\middle|St\big(t + (j\Delta t)\big) \neq St\left(t + \big((j-1) \cdot \Delta t\big)\right)\right\}, \quad j = \overline{1;J}, \tag{1.16}$$

где J – число возможных состояний АСУ; Δt – временной интервал перехода АСУ из одного состояния в другое.

В общем случае множество St можно описать следующим образом:

$$St = \{St(t_1);\ St(t_2); St(t_3); \ldots; St(t_J)\}, \tag{1.17}$$

где t_1, t_2, t_3, ..., t_J – моменты перехода АСУ из одного состояния в другое.

Будем считать, что АСУ находится в безопасном состоянии, если все ее пассивные объекты находятся в безопасном состоянии и, соответственно, множество $St_{\text{безоп}}$ безопасных состояний АСУ – это множество состояний АСУ, в которых все пассивные объекты находятся в безопасном состоянии.

Определение 1.5. Безопасным состоянием i-го пассивного объекта в момент времени t (исходя из определения 1.2) будем считать такое его состояние, при котором все активные объекты, совершающие операции над данным пассивным объектом (в момент времени t) входят во множество разрешенных активных объектов для данного пассивного объекта:

$$\hat{Q}_i(t) \subseteq Q_{\text{акт}_i}; \tag{1.18}$$

каждая операция, совершаемая k-м активным объектом в отношении i-го пассивного объекта (в момент времени t) входит во множество разрешенных операций для данного пассивного объекта:

$$o_{ki}^{(t)} \in O_{ki}; \tag{1.19}$$

число одновременно совершаемых операций в отношении данного пассивного объекта не превышает заранее определенного допустимого значения:

$$n_{\text{оп}_i} \leq N_{\text{зад}_i}. \tag{1.20}$$

Множество $St_{\text{оп}}$ опасных состояний АСУ, в свою очередь, это множество состояний, в которых хотя бы один пассивный объект находится в опасном состоянии.

При этом, пассивный объект находится в опасном состоянии если не выполняется хотя бы одно условие его безопасного состояния (1.18), (1.19), (1.20).

Таким образом, множество состояний АСУ можно представить как:

$$St = St_{\text{безоп}} \cup St_{\text{оп}}, \quad (1.21)$$

при этом:

$$St_{\text{безоп}} \cap St_{\text{оп}} = \emptyset. \quad (1.22)$$

Переход любого пассивного объекта АСУ в опасное состояние означает переход всей АСУ в опасное состояние.

Определение 1.6. Угрозой безопасности АСУ будем называть совокупность условий и факторов, создающих потенциально или реально существующую опасность нарушения безопасности информации или безопасности функционирования АСУ.

При этом, под нарушением безопасности информации в АСУ понимается нарушение хотя бы одного свойства безопасности информации (конфиденциальности, доступности и целостности) [32], а под нарушением безопасности функционирования АСУ – нарушение штатного режима функционирования АСУ и управляемого (контролируемого) объекта и (или) процесса [130].

Описание способа реализации угрозы обычно сводится к описанию канала реализации угрозы, т. е. канала несанкционированного доступа или канала несанкционированного воздействия.

Канал несанкционированного доступа – это совокупность субъекта несанкционированного доступа, объекта несанкционированного доступа и среды доступа [143].

Каналы несанкционированного доступа в операционную среду или непосредственно к информации одновременно могут быть (но не обязательно) возможными каналами несанкционированного воздействия, при этом такие каналы определяются аналогичным образом, т. е. как совокупность субъекта несанкционированного воздействия, объекта несанкционированного воздействия и среды воздействия [143].

С учетом изложенного может быть построена иерархия угроз выполнения действий, направленных на получение доступа к элементам АСУ, затем доступа к информации и, далее, угроз выполнения несанкционированных действий [143] (рисунок 1.4).

Таким образом, представленная иерархия включает в себя:

– угрозы непосредственного (локального) и удаленного доступа в операционную среду компонентов АСУ, а также угрозы несанкционированного воздействия на компоненты АСУ по сети;

– угрозы выполнения деструктивных действий с компонентами АСУ и информационными ресурсами АСУ (хранящейся и обрабатываемой информацией): угрозы нарушения конфиденциальности, целостности и доступности, а также угрозы раскрытия особенностей построения АСУ (например, за счет нарушения конфиденциальности технологической информации, необходимой для функционирования АСУ), и угрозы нарушения штатного режима функционирования АСУ (например, за счет нарушения целостности программных компонентов АСУ).

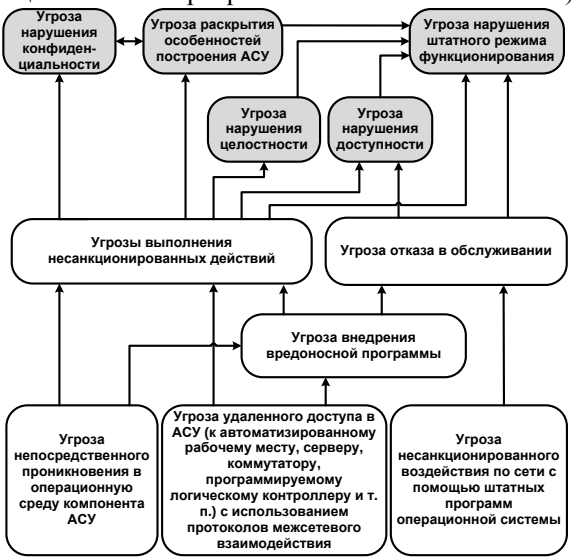


Рисунок 1.4 – Иерархия угроз безопасности АСУ

При определении угроз безопасности АСУ необходимо учитывать структурно-функциональные характеристики защищаемой автоматизированной системы, включающие наличие уровней (сегментов) ее построения; состав защищаемой автоматизированной системы; физические, логические, функциональные и технологические взаимосвязи в защищаемой автоматизированной системе; взаимодействие с иными

автоматизированными системами и информационно-телекоммуникационными сетями; режимы функционирования защищаемой автоматизированной системы, а также иные особенности ее построения и функционирования.

В качестве примеров угроз безопасности АСУ можно привести следующие угрозы [5] (в скобках указан идентификатор угрозы):

1. Для угроз нарушения конфиденциальности:

– угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение (УБИ.77);

– угроза обхода некорректно настроенных механизмов аутентификации (УБИ.100);

– угроза общедоступности облачной инфраструктуры (УБИ.101);

– угроза перехвата данных, передаваемых по вычислительной сети (УБИ.116);

– угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика (УБИ.193).

2. Для угроз раскрытия особенностей построения АСУ:

– угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб (УБИ.98);

– угроза обнаружения хостов (УБИ.99);

– угроза определения типов объектов защиты (УБИ.103);

– угроза определения топологии вычислительной сети (УБИ.104).

3. Для угроз нарушения целостности:

– угроза искажения вводимой и выводимой на периферийные устройства информации (УБИ.27);

– угроза использования поддельных цифровых подписей BIOS (УБИ.32);

– угроза нарушения целостности данных кэша (УБИ.43)

– угроза подмены содержимого сетевых ресурсов (УБИ.130);

– угроза потери информации вследствие несогласованности работы узлов хранилища больших данных (УБИ.136).

4. Для угроз нарушения доступности:

– угроза длительного удержания вычислительных ресурсов пользователями (УБИ.14);

– угроза избыточного выделения оперативной памяти (УБИ.22);

– угроза исчерпания вычислительных ресурсов хранилища больших данных (УБИ.38);

– угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов (УБИ.59).

5. Для угроз нарушения штатного режима функционирования АСУ:

– угроза отключения контрольных датчиков (УБИ.107);

– угроза передачи запрещённых команд на оборудование с числовым программным управлением (УБИ.112);

– угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации (УБИ.143);

– угроза перехвата управления автоматизированной системой управления технологическими процессами (УБИ.183);

– угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров (УБИ.204).

Компьютерная атака является одним из способов реализации угроз безопасности автоматизированной системы управления.

Определение 1.7. Компьютерной атакой на АСУ назовем такое программное воздействие $Imp(t_j)$ на хотя бы один пассивный объект АСУ в момент времени t_j, которое переводит АСУ из безопасного состояния в опасное, либо оставляет АСУ в ранее достигнутом опасном состоянии (понятие программного воздействия будет уточнено ниже).

Таким образом, множество компьютерных атак K может быть представлено как:

$$K = \{Imp(t_j) | St(t_j) \in St_{\text{оп}}\}, j = \overline{1; J}. \quad (1.23)$$

Исходя из анализа различных видов информационно-технических воздействий (в том числе и компьютерных атак) [18, 38, 38, 57, 71, 72, 73, 74, 78, 86, 91, 108, 143] на различные информационно-вычислительные и автоматизированные системы в локальных и региональных вычислительных сетях, а также в сети

Интернет все виды реализации компьютерных атак можно обобщить так, как показано на рисунке 1.5.

При этом можно выделить две группы компьютерных атак [143]:

- пассивные компьютерные атаки;
- активные компьютерные атаки.



Рисунок 1.5 – Основные виды компьютерных атак

Пассивной компьютерной атакой называют такую атаку, которая не оказывает непосредственного влияния на атакуемую автоматизированную систему управления, но при этом, с ее помощью возможны реализации угроз безопасности АСУ (в частности угрозы нарушения конфиденциальности информации, обрабатываемой и хранимой в атакуемой АСУ или угрозы раскрытия особенностей построения атакуемой АСУ).

Под активной компьютерной атакой понимается атака, оказывающая непосредственное влияние на атакуемую автоматизированную систему управления и позволяющая реализовать угрозы безопасности АСУ.

Более подробно виды и способы реализации компьютерных атак, а также угрозы, на реализацию которых направлены эти атаки представлены в приложении А (таблица А.1).

Возможность реализации угроз безопасности АСУ с помощью компьютерных атак определяется наличием различных дефектов [10, 11, 70, 83, 93] безопасности в компонентах защищаемой автоматизированной системы (рисунок 1.6).



Рисунок 1.6 – Виды дефектов безопасности АСУ

Определение 1.8. Под дефектом безопасности АСУ будем понимать недостаток (ошибку) проектирования и (или) создания программных (программно-технических) компонентов АСУ потенциально влияющий на ее безопасность.

Определение 1.9. Под уязвимостью АСУ будем понимать такой дефект безопасности АСУ, использование (эксплуатация) которого может привести к реализации угрозы безопасности АСУ.

При этом следует отметить, что для эксплуатации дефекта безопасности необходимо наличие субъекта (нарушителя), воздействующего на автоматизированную систему, обладающего определенными возможностями (компетенция, оснащенность, мотивация) [54] (рисунок 1.7).

Любая (*i*-я) угроза безопасности АСУ характеризуется вероятностью $P_{\text{УГР}_{ij}}$ ее реализации в отношении *j*-го пассивного объекта АСУ и возможным ущербом U_j от перехода *j*-го объекта (и

соответственно всей автоматизированной системы) в опасное состояние.

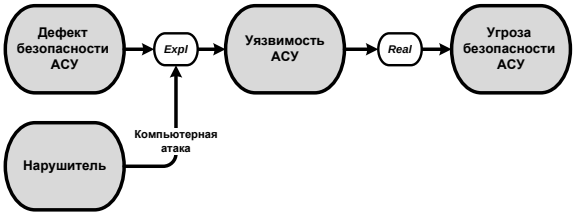


Рисунок 1.7 – Эксплуатация (*Expl*) дефекта безопасности АСУ нарушителем для реализации (*Real*) угрозы безопасности

Вероятность реализации i-й угрозы в отношении j-го пассивного объекта зависит от потенциала нарушителя $Pt_{\text{нар}}$ и степени опасности η_{ij} уязвимости, имеющейся в j-м объекте АСУ и позволяющей реализовать i-ю угрозу (рисунок 1.8):

$$P_{\text{УГР}_{ij}} = f(Pt_{\text{нар}}, \eta_{ij}). \tag{1.24}$$

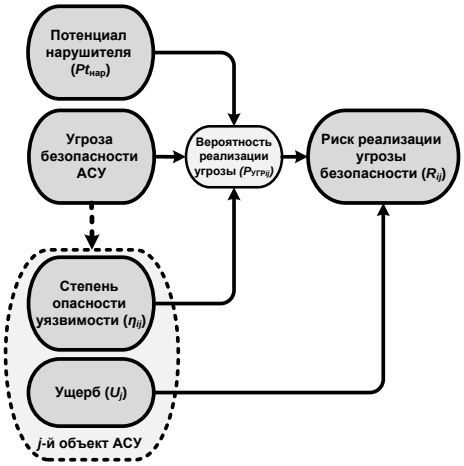


Рисунок 1.8 – Взаимосвязь потенциала нарушителя, степени опасности уязвимости, ущерба, вероятности реализации угрозы и риска реализации угрозы

Определение 1.10. Риском реализации i-й угрозы в отношении j-го объекта АСУ будем называть произведение вероятности

реализации *i*-й угрозы в отношении *j*-го объекта на ущерб от перехода *j*-го объекта в опасное состояние [4, 69, 98, 125]:

$$R_{ij} = P_{\text{УГР}_{ij}} U_j. \quad (1.25)$$

В определении 1.7 компьютерная атака определена как программное воздействие на пассивный объект АСУ, т. е. воздействие на пассивный объект АСУ с помощью какой-либо отдельной программы или программы, входящей в состав какого-либо программно-технического средства.

Определение 1.11. Под программным воздействием на пассивный объект АСУ будем понимать воздействие на этот объект с помощью программы pr_{imp}, такой что:

$$\left(F(pr_{imp}) \subset F_{imp}\right) \wedge \left(F(pr_{imp}) \neq \emptyset\right), \quad (1.26)$$

где $F(pr_{imp})$ – функции выполняемые программой pr_{imp}, F_{imp} – множество функций информационно-технического воздействия, таких как [85, 112]:

– сокрытие признаков своего присутствия в системе;

– самодублирование, в том числе создание модифицированных своих копий;

– ассоциирование себя с другими программами;

– перенос своих фрагментов в иные области оперативной или внешней памяти, в том числе находящиеся на удаленном компьютере;

– получение несанкционированный доступ к компонентам или ресурсам системы;

– разрушение или искажение кода программ в оперативной памяти;

– наблюдение за процессами обработки информации и принципами функционирования средств защиты;

– сохранение фрагментов информации из оперативной памяти в некоторой области внешней памяти;

– искажение, блокирование или подмена выводимого во внешнюю память, на автоматизированное рабочее место или канал связи информационного массива, образовавшегося в результате работы прикладных программ;

– искажение находящихся во внешней памяти массивов данных;

– нейтрализация работы тестовых программ и средств защиты информационных ресурсов системы;

– постоянное или кратковременное изменение степени защищенности конфиденциальных данных;

– перевод в неработоспособное состояние или разрушение компонентов системы;

– создание скрытых каналов передачи данных;

– инициирование ранее внедренных разрушающих программных воздействий.

В общем, множество программ $Pr_{imp} = \{pr_{imp_1}; pr_{imp_2}; pr_{imp_3}; \dots; pr_{imp_{N_{pr}}}\}$, с помощью которых можно осуществлять воздействие на объекты АСУ, включает в себя два подмножества: подмножество Pr_{mal} вредоносных программ, специально созданных для осуществления вредоносных функций и подмножества Pr_{sw} программ, изначально созданных для выполнения вполне легальных действий, но с помощью которых также можно осуществлять воздействие на объекты АСУ (например различные утилиты сканирования сетей и анализа сетевого трафика, отладчики или HEX-редакторы).

Т. е. множество программ Pr_{imp} можно описать следующим образом:

$$Pr_{imp} = Pr_{mal} \cup Pr_{sw}, \tag{1.27}$$

при этом:

$$Pr_{mal} \cap Pr_{sw} = \emptyset. \tag{1.28}$$

Для определения понятия «вредоносная программа» целесообразно воспользоваться подходом, основанном на представлении вредоносных программ на функциональном уровне, т. е. в виде функциональных элементов, определяющих их действия [49].

Всего можно выделить три типа функциональных элементов, определяющих действия таких программ:

– функциональный элемент, реализующий функцию ущерба;

– функциональный элемент, реализующий функцию размножения;

– функциональный элемент, реализующий функцию преодоления средств защиты.

Функцию нанесения ущерба определим, как функцию, предназначенную для осуществления несанкционированного доступа к информации и (или) несанкционированного воздействия на информацию или компоненты автоматизированной системы управления, под которым понимается уничтожение, блокирование, модификация либо копирование информации, а также нарушение работы отдельных компонентов автоматизированной системы управления или автоматизированной системы управления в целом.

Функцию размножения определим, как функцию, предназначенную для внедрения копии вредоносной программы или участка вредоносного программного кода в заражаемую программу или в вычислительную систему. При этом внедренные копии вредоносной программы могут быть модифицированы, и сохранять способность к дальнейшему размножению.

Функцию преодоления средств защиты определим, как функцию, предназначенную для совершения действий, запрещаемых средствами защиты (получение неавторизованного доступа, подбор паролей, получение доступа к защищенным файлам и т. п.).

Введем обозначения:

- F_{dam} – множество функций нанесения ущерба;
- F_{rep} – множество функций размножения;
- F_{ov} – множество функций преодоления защиты.

Определение 1.12. Под вредоносной программой будем понимать такую программу pr, которая реализует хотя бы одну функцию из множества $F_{mal} = F_{dam} \cup F_{rep} \cup F_{ov}$.

Таким образом, множество вредоносных программ M_{pr} можно определить как:

$$M_{pr} = \{pr | f_{pr} \in (F_{mal} \cap F(pr))\}, \quad (1.29)$$

где f_{pr} – функция программы pr; $F(pr)$ – множество функций программы pr.

При этом, можно выделить три основных вида вредоносных программ [51, 85]:

– компьютерные вирусы;
– троянские программы;
– черви.

Положение 1.1. Необходимым и достаточным условием для признания какой-либо программы pr вирусом является наличие в ее составе функции размножения путем внедрения собственного кода в другие программы, файлы и (или) системные области вычислительных средств:

$$\left(pr \in Vir_{pr}\right) \Leftrightarrow \left(f_{pr} \in (F_{rep} \cap F(pr))\right), \quad (1.30)$$

где Vir_{pr} – множество компьютерных вирусов.

Положение 1.2. Необходимым условием для признания какой-либо программы pr троянской является наличие функции нанесения ущерба:

$$\left(pr \in Troj_{pr}\right) \Rightarrow \left((F(pr) \cap F_{dam}) \neq \emptyset\right), \quad (1.31)$$

а достаточным условием – отсутствие функции размножения путем внедрения собственного кода в другие программы, файлы и (или) системные области вычислительных средств:

$$\left((F(pr) \cap F_{dam}) = \emptyset\right) \Rightarrow \left(pr \in Troj_{pr}\right), \quad (1.32)$$

где $Troj_{pr}$ – множество троянских программ.

Положение 1.3. Необходимым и достаточным условием для отнесения программ к классу червей является наличие в его составе функции преодоления средств защиты:

$$\left(pr \in Worm_{pr}\right) \Leftrightarrow \left(f_{pr} \in (F(pr) \cap F_{ov})\right), \quad (1.33)$$

где $Worm_{pr}$ – множество программ типа «червь».

Определение 1.13. Средство защиты s от компьютерных атак – техническое, программное, программно-техническое средство, предназначенное или используемое для защиты компонентов и (или) информационных ресурсов автоматизированной системы управления от компьютерных атак.

Определение 1.14. Системой защиты автоматизированной системы управления в целом или отдельных ее составляющих от компьютерных атак называется множество

$$S = \{s_1, s_2, \dots, s_J\}, \quad (1.34)$$

где s_j – отдельное средство защиты от компьютерных атак, при $j = \overline{1;J}$, элементы которого (в совокупном единстве) обеспечивают защиту от компьютерных атак.

При этом защита от компьютерных атак подразумевает под собой обнаружение компьютерных атак, противодействие компьютерным атакам, устранение последствий компьютерных атак.

Определение 1.15. Под обнаружением компьютерной атаки понимается установление факта проведения компьютерной атаки в отношении автоматизированной системы управления, а также выявление источника (субъекта) и средств реализации компьютерной атаки в отношении автоматизированной системы управления.

Определение 1.16. Под противодействием компьютерной атаке понимается создание системой защиты таких условий, в которых компьютерная атака, даже будучи реализованной, не сможет достичь своих целей.

Определение 1.17. Под устранением последствий компьютерной атаки понимается блокировка источника (субъекта) атаки, нейтрализация средства реализации компьютерной атаки (удаление его из оперативной и (или) внешней памяти компонентов автоматизированной системы управления или его изоляция) и (или) восстановление автоматизированной системы управления в состояние до реализации компьютерной атаки.

Далее предполагается, что каждое средство защиты s проявляет свои защитные свойства за счет реализации некоторого множества функций, которое будет обозначаться через $F(s)$. Пример множества реализуемых функций для средств антивирусной защиты приведен в приложении Б.

1.3 Модели защиты от компьютерных атак

Моделирование какой-либо системы или процесса заключается в построении некоторого ее образа, адекватного (с точностью достаточной для целей моделирования) исследуемой

системе, и получения с помощью построенной модели необходимых характеристик поведения реальной системы.

Модель защиты автоматизированной системы от компьютерных атак это абстрактное (формализованное или неформализованное) описание комплекса программно-технических средств или организационных мер защиты (обнаружение, противодействие, устранение последствий) от компьютерных атак [120].

В самом общем виде модель процесса защиты может быть представлена так, как показано на рисунке 1.9 [25, 69, 138].

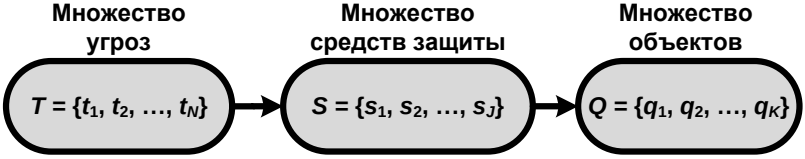


Рисунок 1.9 – Общая модель процесса защиты от компьютерных атак

Данная модель носит название «формальная модель безопасности с полным перекрытием». В модели рассматривается взаимодействие «защищаемой области», «области угроз» и «средств обеспечения безопасности»:

– $T = \{t_1; t_2; \dots t_N\}$ – множество угроз безопасности;

– $S = \{s_1; s_2; \dots s_J\}$ – множество средств обеспечения безопасности;

– $Q = \{q_1; q_2; \dots q_K\}$ – множество объектов защиты.

Элементы этих множеств находятся между собой в определенных отношениях, для описания которых целесообразно использовать графовое представление (рисунок 1.6).

Множество отношений «угроза-объект» описывается двудольным графом TQ. Цель защиты состоит в том, чтобы перекрыть все возможные ребра в графе. Это достигается введением третьего множества S, в результате чего получается трехдольный граф TSQ. В защищенной системе все ребра графа представляются в виде $< t_n ; s_j >$ и $< s_j; q_k >$. Любое ребро $< t_n; q_k >$ определяет незащищенный объект (ребро $< t_2; q_3 >$ на рисунке 1.10).

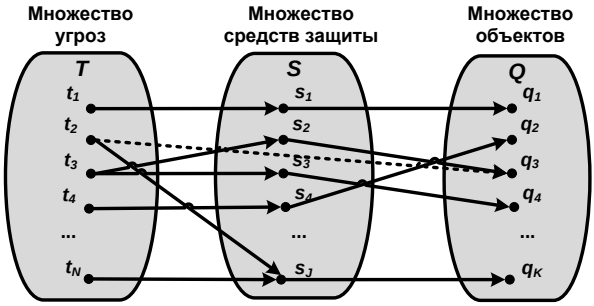


Рисунок 1.10 – Графовое представление отношений между множествами угроз безопасности, средств обеспечения безопасности, объектов защиты

В модели безопасности с полным перекрытием выполняется условие полной защищенности:

$$\forall t_n \in T, \exists s_j \in S, \tag{1.35}$$

означающее, что для каждой угрозы t_n из множества угроз T существует средство обеспечения безопасности s_j из множества S, перекрывающее путь реализации этой угрозы к объекту защиты q_k.

Расширение представленной модели с полным перекрытием предполагает включение множества уязвимостей объектов автоматизированной системы и множества барьеров, представляющие собой пути реализации угроз, перекрытые средствами защиты [4, 69]. Помимо множеств уязвимостей и барьеров в расширенную модель включено множество компьютерных атак, которые являются способом реализации угроз в отношении объектов АСУ.

Данная модель может быть представлена в виде графа $Pr = \{K, T, S, B, V, Q\}$ (рисунок 1.11), где K – множество компьютерных атак; T – множество угроз, S – множество средств защиты; Q – множество объектов защиты (компонентов и информационных ресурсов) автоматизированной системы управления; $V = KTQ = \{v_l =< k_m; t_i; q_n >, l = \overline{1; L}\}$ – множество уязвимостей объектов АСУ, представляющих собой путь реализации *i*-й угрозы в отношении *j*-го объекта с помощью *m*-ой компьютерной атаки; $B = VS = KTQS = \{b_k =< k_m; t_i; q_n; s_j >,$

$k = \overline{1;K}\}$ – множество барьеров, в которых требуется осуществлять защиту.

Для данной модели условие полного перекрытия описывается следующим образом:

$$\forall v_l \in V, \exists\left(b_k =< k_m t_i q_n s_j >\right) \in B. \quad (1.36)$$

Данное условие означает, что для каждой уязвимости v_l из множества V средством защиты s_j из множества S создается барьер b_k из множества B, тем самым устраняя уязвимость v_l, что делает невозможным реализацию угрозы t_i из множества T компьютерной атакой k_m из множества K.

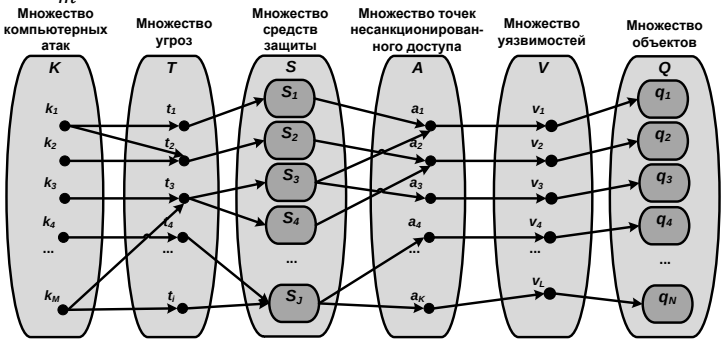


Рисунок 1.11 – Расширенная модель защиты от компьютерных атак, учитывающая уязвимости и барьеры

Расширенная модель защиты с полным перекрытием, несмотря на ее корректность с формальной точки зрения, обладает существенными ограничениями для ее практического применения, основными из которых являются [4, 69]:

– сложность идентификации полного множества угроз и уязвимостей для конкретной автоматизированной системы;

– отсутствие возможности количественной оценки уровня защищенности;

– отсутствие возможности проведения анализа безопасности по критерию «эффективность-стоимость».

Для преодоления отмеченных трудностей на практике используются два подхода: нормативно-гарантированный (классификационный) и основанный на анализе риска (риск-ориентированный).

1.3.1 Модель защиты от компьютерных атак на основе нормативно-гарантированного подхода

Нормативно-гарантированный подход основывается на нескольких базовых нормативно-методических документах [92, 116, 119, 121, 123, 130 ,135].

Руководящий документ [116] определяют девять классов защищенности автоматизированных систем, объединенные в три группы в соответствии с особенностями обработки информации и функционирования АСУ. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности автоматизированных систем (рисунок 1.12). Каждому классу поставлен в соответствие набор обязательных требований по обеспечению защищенности АСУ.

В руководящих документах [92, 130, 135] предлагается классифицировать защищаемую систему по классам защищенности. Так, руководящий документ [130] предполагает три класса защищенности, которые определяются в зависимости от уровня значимости (критичности) обрабатываемой в защищаемой системе информации, документы [92, 135] – четыре класса защищенности, которые определяются в зависимости от уровня значимости (критичности) информации, обрабатываемой в защищаемой системе, и масштаба защищаемой системы (федеральный, региональный, объектовый). Далее, в указанных документах, для каждого класса защищенности определены меры защиты, подлежащие выполнению (при этом технические меры реализуются соответствующими средствами защиты).

При таком подходе функциональным критерием обеспечения безопасности АСУ является выполнение заданного набора требований (гарантированной защиты): $F_{\text{зад}} \subseteq \bigcup_{j=1}^{J} F(S_j)$, где $F_{\text{зад}}$ – заданный набор требований к системе защиты от компьютерных атак, $F(S_j)$ – множество функций, реализуемых j-м средством защиты, входящим в систему защиты, J – число средств защиты, входящих в систему защиты от компьютерных атак; а критерием экономической эффективности минимальные суммарные затраты на их реализацию: $\sum_{j=1}^{J} C(S_j) \to min$, где $C(S_j)$ – стоимость j-го

средства защиты, входящего в состав системы защиты от компьютерных атак, $j = \overline{1;J}$.

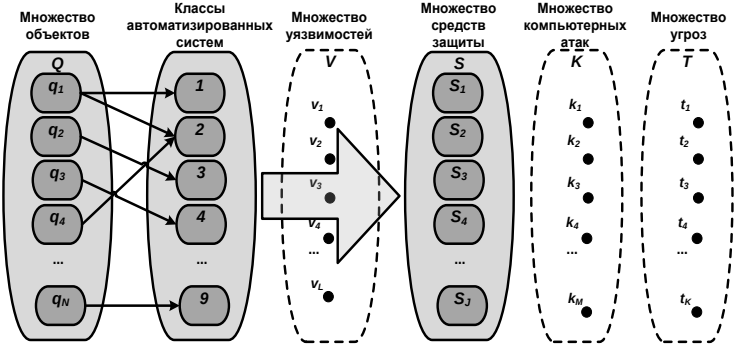


Рисунок 1.12 – Модель защиты от компьютерных атак на основе нормативно-гарантированного подхода

Данный подход обладает следующими достоинствами [51, 69]:

– обеспечивает в соответствующем классе одинаковый уровень безопасности объектов для различных организаций на основе универсальности и возможности реализации типовых организационно-технических решений;

– отвечает требованиям доступности и массового применения для однотипных по виду предметной деятельности и структуре организаций.

Но при этом нормативно-гарантированный подход имеет и достаточно серьезные недостатки [51, 69]:

– не определяет с функциональной точки зрения точных значений показателей защищенности, хотя и позволяет классифицировать защищаемые автоматизированные системы по уровню безопасности и сравнивать их между собой;

– не отвечает требованиям экономической и ресурсной эффективности.

Помимо этого, следует отметить, что в руководящих документах [92, 130, 135] определены технические меры защиты, которые не отнесены ни к одному из классов защищенности, а необходимость их реализации должна быть определена на этапе проектирования и построения системы защиты исходя из структурно-функциональных характеристик защищаемой системы

и с учетом всех возможных угроз безопасности автоматизированной системы.

1.3.2 Модель защиты от компьютерных атак на основе риск-ориентированного подхода

Приведенные выше недостатки и ограничения нормативно-гарантированного подхода предполагают актуализацию иных подходов к обеспечению безопасности информации в автоматизированных системах управления и безопасного их функционирования и формированию требований к этим системам в части касающейся защиты от компьютерных атак, в том числе базирующихся на идее соразмерности защиты и масштабов угроз [7, 8, 69, 110].

Для расширенной модели с полным перекрытием (рисунок 1.11) в качестве характеристик элемента $b_k =< k_m; t_i; q_n; s_j >$ множества барьеров B может рассматриваться пара $\{p_k; u_k\}$, где p_k – вероятность реализации угрозы t_i с помощью компьютерной атаки k_m в отношении объекта q_n; u_k – возможный ущерб от реализации угрозы t_i в отношении объекта q_n.

Вероятность p_k зависит от потенциала возможного нарушителя безопасности [54, 51] и степени опасности уязвимости v_l, закрываемой барьером b_k (исходя из (1.24) и (1.36)):

$$p_k = f(Pt, \eta_k), \tag{1.37}$$

где Pt – потенциал нарушителя безопасности; η_k – степень опасности уязвимости [1], закрываемой барьером b_k.

Как известно, деятельность, которая сопровождается вероятным появлением ущерба, считается рисковой, а риском в данном контексте является мера, учитывающая вероятность реализации угрозы и величину ущерба (потерь) от ее реализации.

Таким образом, исходя из (1.25) для объекта q_n риск r_k нанесения ущерба u_k, в случае реализации угрозы t_i будет представлен следующим выражением:

$$r_k = p_k \times u_k. \tag{1.38}$$

Как видно, × – это обычное произведение вероятности на количественное выражение ущерба, т. е. в определенном смысле риск r_k – это математическое ожидание ущерба u_k.

Тогда необходимую эффективность барьера b_k, создаваемого с помощью средства защиты s_j можно определить как функцию от риска r_k:

$$E(b_k) = f(r_k). \tag{1.39}$$

Учитывая, что барьер b_k создается с помощью средства защиты s_j можно от эффективности барьера $E(b_k)$ перейти к эффективности средства защиты $E(s_j)$ и тогда:

$$E(s_j) = f(r_k). \tag{1.40}$$

В свою очередь затраты на средство защиты зависят от его эффективности: чем выше эффективность средства защиты, тем выше затраты (рисунок 1.13).

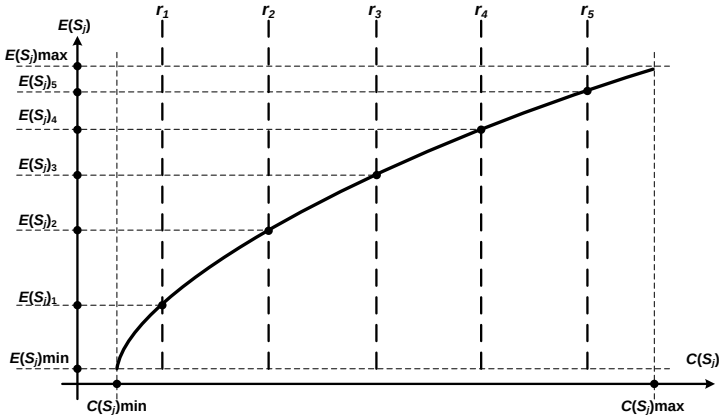


Рисунок 1.13 – Зависимость затрат от эффективности для средства защиты от компьютерных атак

Если риск r_k нанесения ущерба u_k, в случае реализации угрозы t_i в отношении объекта q_n посредством компьютерной атаки k_m минимален, то соответственно для реализации барьера b_k достаточно средства защиты s_j с минимальной эффективностью, которое будет наименее затратно:

$$(r_k = min) \Rightarrow (E(s_j) = min) \Rightarrow (C(s_j) = min). \quad (1.41)$$

Если же риск r_k нанесения ущерба u_k, в случае реализации угрозы t_i в отношении объекта q_n посредством компьютерной атаки k_m максимален, то соответственно для реализации барьера b_k необходимо средство защиты s_j с максимальной эффективностью и, которое будет иметь максимальную стоимость:

$$(r_k = max) \Rightarrow (E(s_j) = max) \Rightarrow (C(s_j) = max). \quad (1.42)$$

На рисунке 1.9 показаны пять значений риска, такие что:

$$r_1 < r_2 < r_3 < r_4 < r_5. \quad (1.43)$$

Тогда, исходя из (1.41) и (1.42):

$$E(s_j)_1 < E(s_j)_2 < E(s_j)_3 < E(s_j)_4 < E(s_j)_5 \quad (1.44)$$

и

$$C(s_j)_1 < C(s_j)_2 < C(s_j)_3 < C(s_j)_4 < C(s_j)_5. \quad (1.45)$$

Таким образом, путем оценки риска для каждой возможной угрозы из множества T, возможно определение минимально необходимой (достаточной) эффективности для каждого средства защиты из множества S.

Исходя из (1.44) и (1.45) возможна реализация системы защиты с минимальными затратами, которая в свою очередь будет обеспечивать уровень защиты от компьютерных атак адекватный возможным рискам нарушения безопасности функционирования АСУ в условиях воздействия на нее компьютерных атак.

1.4 Стратегии защиты от компьютерных атак

Стратегия защиты от компьютерных атак – кратко выраженная целеполагающая идея, определяющая направленность и характер проводимых мероприятий по защите АСУ от компьютерных атак, состав и характеристики применяемых мер и средств защиты [141].

Классификация известных на сегодняшний день стратегий защиты приведена на рисунке 1.14.



Рисунок 1.14 – Классификация стратегий защиты автоматизированных систем управления [141]

Стратегия "периметровой" защиты заключается в том, что АСУ защищается по ее периметру от внешних информационных воздействий, а также от угроз несанкционированной передачи защищаемой информации из защищаемой АСУ в сеть общего пользования.

Реализация стратегии «периметровой» защиты в автоматизированных системах управления осуществляется с помощью программных и программно-аппаратных средств защиты, способным организовать ограничение потока данных, фильтрацию и анализ пакетов и процессов. К данным средствам относятся [107]:

– межсетевые экраны (файерволы), контролирующие по определенным правилам входящий и выходящий трафик АСУ;

– фильтры содержимого (контента), способные проанализировать входящую информацию и принять соответствующие действия;

– системы обнаружения вторжений, выявляющие факты неавторизованного доступа в сеть либо несанкционированного управления системой;

– внешние шлюзы, выполняющие функции маршрутизатора и др.

Стратегия эшелонированной защиты АСУ заключается в том, что защита реализуется на нескольких уровнях [9, 141]:

– по периметру;
– на уровне серверов сети;
– на уровне рабочих станций (автоматизированных рабочих мест);
– на уровне операционной системы каждого хоста;
– на уровне приложений (прикладных программ);
– на уровне архитектуры программно-аппаратной среды.

Применительно к автоматизированным системам управления технологическими процессами, построение эшелонированной системы защиты возможно по периметру автоматизированной системы и на каждом уровне построения защищаемой системы (уровне операторского управления, уровне автоматического управления, уровне ввода (вывода) данных).

Сущность выборочной стратегии (или стратегии «ключевых элементов») заключается в защите наиболее важных элементах (программных или программно-аппаратных компонентах) защищаемой системы [141]. Данная стратегия применяется в случае, если существуют какие-либо ограничения на состав применяемых мер и средств защиты.

Стратегия тотального контроля заключается в том, что осуществляется контроль любых действий, операций, команд в автоматизированной системе. При этом возможны два пути реализации данной стратегии [141, 143].

Первый путь заключается в контроле всех действий, операций, команд специально выделенным программным (программно-аппаратным) монитором безопасности. Такой контроль может осуществляться на прикладном уровне (путем перехвата системных функций прикладного уровня), либо на уровне ядра операционной системы (например, путем внесения изменений в таблицу дескрипторов системных вызовов) [58].

Второй путь заключается в том, что по всей автоматизированной системе устанавливаются программные (программно-аппаратные) «агенты», осуществляющие выявление любых аномалий (аномалий трафика по периметру сети, нарушений правил разграничения доступа на рабочих местах операторов АСУ, сигнатур вредоносных программ и т. п.) [39, 141, 143].

Стратегия пресечения является на сегодняшний день основной, широко применяемой на практике. Данная стратегия направлена на пресечение всех возможных попыток нарушителя реализовать угрозы безопасности АСУ.

Помимо стратегии пресечения возможна реализация стратегии обмана (отвлечения нарушителя) и стратегии маскировки.

Стратегия обмана, заключается в отвлечении нарушителя на специально создаваемые ложные элементы автоматизированной системы управления. К примеру, в руководящих документах [92, 130, 135] данную стратегию предлагается реализовывать путем:

– создания (эмуляции) ложных компонентов автоматизированной системы управления, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности информации;

– воспроизведения ложных отдельных информационных технологий и (или) структурно-функциональных характеристик автоматизированной системы управления или ее сегментов, обеспечивающих навязывание нарушителю ложного представления об истинных информационных технологиях и (или) структурно-функциональных характеристиках автоматизированной системы управления.

Стратегия маскировки заключается в скрытии информационных технологий и (или) структурно-функциональных характеристик автоматизированной системы управления [68], а также в преобразовании информации, хранимой и обрабатываемой в автоматизированной системе управления информации, вследствие которого она становится недоступной для нарушителя.

Примером реализации данной стратегии является механизм рандомизации адресного пространства оперативной памяти (ASLR – Address Space Layout Randomization) [124], а также использование различных криптографических и стеганографических алгоритмов [14, 30, 31].

По признаку превентивности защиты могут применяться стратегии, направленные на предупреждение возникновения и реализации той или иной угрозы, на игнорирование угроз и последствий их реализации (когда экономически более целесообразно признается, например восстановление информации, после реализации угроз) и на своевременное выявление и отслеживание факта реализации угрозы [141, 143].

По адаптивности, системы защиты могут быть неадаптивными (т. е. не иметь возможности изменять какие-либо свои характеристики, в зависимости от складывающейся ситуации) и адаптивными. В современных системах защиты данная стратегия, как правило, реализуется в виде возможных заранее предусмотренных вариантов действий. К примеру, в [130] определена такая мера защиты, как «перевод автоматизированной системы или ее устройств (компонентов) в заранее определенную конфигурацию, обеспечивающей защиту, в случае возникновения отказов (сбоев)».

По признаку активности защиты, стратегии делятся на те, которые предполагают применение только активных или только пассивных средств защиты, и те, которые сочетают активные и пассивные средства [141, 143].

Далее, в работе материал будет излагаться преимущественно для эшелонированных (в соответствии с иерархической (многоуровневой) структурой защищаемых АСУ (рисунок 1.2)) систем защиты, основанной на стратегии пресечения с отдельными элементами стратегий обмана и маскировки и с возможностью адаптации путем перевода автоматизированной системы или ее компонентов в заранее определенные конфигурации.

1.5 Постановка задачи выбора оптимального варианта построения системы защиты от компьютерных атак

Согласно нормативных и методических документов по построению автоматизированных систем в защищенном исполнении [120, 123, 128, 130, 132] технические меры (способы) защиты, реализуемые в автоматизированной системе в рамках ее системы защиты обеспечиваются следующими средствами:

– средства идентификации и аутентификации субъектов доступа и объектов доступа;

– средства управления доступом субъектов доступа к объектам доступа;

– средства ограничения программной среды;

– средства защиты машинных носителей информации;

– средства регистрации событий безопасности;

– средства антивирусной защиты;

– средства обнаружения (предотвращения) вторжений;

– средства контроля (анализа) защищенности информации;

– средства обеспечения целостности автоматизированной системы управления и информации;

– средства обеспечения доступности технических средств и информации;

– средства защиты среды виртуализации;

– средства защиты технических средств и оборудования автоматизированной системы;

– средства защиты автоматизированной системы и ее компонентов (в том числе и средства эмуляции ложных компонентов автоматизированной системы, предназначенных для обнаружения, регистрации и анализа действий нарушителей в процессе реализации угроз безопасности, а также средства воспроизведения ложных и (или) скрытие истинных отдельных технологий и (или) структурно-функциональных характеристик автоматизированной системы управления или ее сегментов, обеспечивающее навязывание нарушителю ложного представления об истинных технологиях и (или) структурно-функциональных характеристиках [92, 130]);

– средства управления обновлениями программного обеспечения автоматизированной системы;

– средства управления конфигурацией автоматизированной системы и ее системы защиты;

– средства криптографической защиты.

Помимо этого реализация технических мер в рамках системы защиты [130]:

– должна обеспечивать доступность обрабатываемой в автоматизированной системе информации (исключение неправомерного блокирования информации), ее целостность (исключение неправомерного уничтожения, модифицирования информации), а также, при необходимости, конфиденциальность (исключение неправомерного доступа, копирования, предоставления или распространения информации);

– должна соотноситься с мерами по промышленной, физической, пожарной, экологической, радиационной безопасности, иными мерами по обеспечению безопасности автоматизированной системы и управляемого (контролируемого) объекта и (или) процесса;

– не должна оказывать отрицательного влияния на штатный режим функционирования автоматизированной системы.

Исходя из указанного, задача выбора оптимального варианта построения системы защиты от компьютерных атак может быть сформулирована следующим образом: выбрать оптимальный вариант построения системы защиты $x_{\text{опт}}$ от компьютерных атак, позволяющий обеспечить минимальное снижение производительности $\Delta\pi$ защищаемой АСУ при обеспечении требуемого уровня защиты E и при ограничениях на стоимость создания системы защиты C:

Таким образом, задача выбора оптимального варианта построения системы защиты в формализованном виде будет выглядеть следующим образом:

$$x_{\text{опт}} = \underset{x_i \in X}{argmin}\, \Delta\pi(x_i), \tag{1.46}$$

$$C(x_i) \leq C_{\text{зад}}, \tag{1.47}$$

$$E(x_i) \geq E_{\text{треб}}, \tag{1.48}$$

где $\Delta\pi$ – показатель, характеризующий степень снижения производительности защищаемой автоматизированной системы; $x_{\text{опт}}$ – оптимальный вариант построения системы защиты от компьютерных атак (т. е. имеющий оптимальную структуру); x_i – возможный вариант построения системы защиты; X – множество возможных вариантов построения системы защиты; $C(x_i)$ – стоимость возможного варианта построения системы защиты; $E(x_i)$ – эффективность возможного варианта построения системы защиты; $C_{\text{зад}}$ – заданная (допустимая) стоимость системы защиты; $E_{\text{треб}}$ – требуемая эффективность системы защиты.

Варьируемыми параметрами в потенциально возможных вариантах построения системы защиты x_i от разрушающих программных воздействий являются:

– состав системы защиты, который описывается в виде множества $S = \{s_1, s_2, \dots, s_J\}$ (определение 1.14);

– множество функций $F(s_i)$, реализуемых каждым средством защиты, входящим в множество S.

Изменение состава системы защиты от компьютерных атак и множеств функций, реализуемых каждым средством ведет к изменению всех вышеописанных показателей.

При этом, с целью уменьшения количества вариантов, упрощения их формирования и проведения расчетов показателей, характеризующих эти варианты, необходимо осуществить декомпозицию задачи выбора оптимального варианта построения системы защиты.

В данном случае декомпозицию задачи выбора оптимального варианта построения системы защиты целесообразно осуществить по последовательности выполнения процедур формирования оптимального варианта построения системы защиты.

Исходя из ограничений (1.47) и (1.48), указанную декомпозицию предлагается осуществить путем решения следующих частных задач (рисунок 1.15):

– формирование множества всех возможных вариантов построения системы защиты;

– формирование множества альтернативных вариантов построения системы защиты;

– формирование множества предпочтительных вариантов построения системы защиты;

– выбор из сформированного множества предпочтительных вариантов, оптимального варианта построения системы защиты.

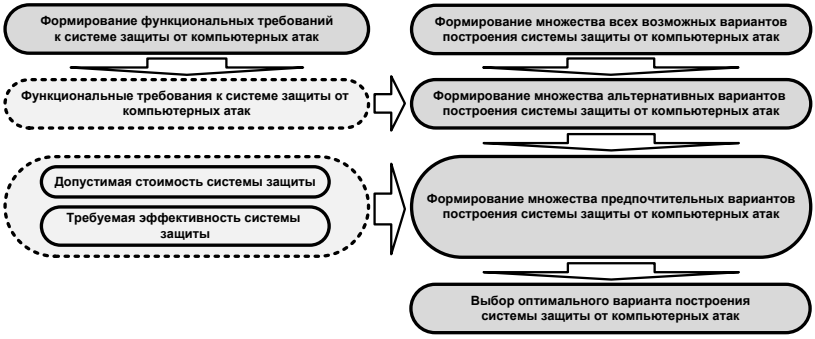


Рисунок 1.15 – Декомпозиция задачи выбора оптимального варианта построения системы защиты от компьютерных атак

Для дальнейшего изложения определим понятия «альтернативный вариант построения системы защиты»,

«предпочтительный вариант системы защиты» и «оптимальный вариант системы защиты» и введем одно положение.

Определение 1.18. Альтернативным вариантом построения системы защиты будем называть такую совокупность средств защиты вида:

$$S = \{s_1; s_2; \dots; s_A\}, \tag{1.49}$$

суммарные функциональные возможности отдельных элементов которой соответствуют заданным функциональным требованиям $F_{\text{зад}}$:

$$F_{\text{зад}} \subseteq \left(F(s_1) \cup F(s_2) \cup \dots \cup F(s_A)\right), \tag{1.50}$$

где $F(s_1), F(s_2), \dots, F(s_A)$ – функции, реализуемые отдельными средствами защиты, а заданные функциональные требования $F_{\text{зад}}$ определяются как множество вида:

$$F_{\text{зад}} = F_{\text{зад}}(s_1) \cup F_{\text{зад}}(s_2) \cup \dots \cup F_{\text{зад}}(s_A), \tag{1.51}$$

где $F_{\text{зад}}(s_1), F_{\text{зад}}(s_2), \dots, F_{\text{зад}}(s_A)$ – функциональные требования к отдельным средствам защиты.

При этом под функциональными требованиями к средству защиты, в данном случае понимается требования, определяющие уровень функциональных возможностей этого средства.

Положение 1.4. Каждое (i-е) средство защиты имеет стоимость $C(s_i)$, а стоимость совокупности средств защиты $C(S)$ определяется как:

$$C(S) = \sum_{i=1}^{A} C\,(s_i). \tag{1.52}$$

где $S = \{s_1, s_2, \dots, s_A\}$, A – число средств защиты в совокупности S

Определение 1.19. Допустимым по стоимости вариантом построения системы защиты будем называть такую совокупность средств защиты вида:

$$S = \{s_1; s_2; \dots; s_A\}, \tag{1.53}$$

которая одновременно удовлетворяет условиям:

$$F_{\text{зад}} \subseteq (F(s_1) \cup F(s_2) \cup \ldots \cup F(S_A)), \tag{1.54}$$

и

$$(C(s_1) + C(s_2) + \cdots + C(s_A)) \leq C_{\text{зад}} \tag{1.55}$$

где $C(s_1), C(s_2), \ldots, C(s_A)$ – стоимости отдельных средств, входящих в совокупность S, $C_{\text{зад}}$ – допустимая стоимость системы защиты.

Определение 1.20. Предпочтительным вариантом построения системы защиты будем называть такую совокупность средств защиты вида:

$$S = \{s_1; s_2; \ldots; s_A\}, \tag{1.56}$$

которая одновременно удовлетворяет условиям:

$$\begin{gathered} F_{\text{зад}} \subseteq \big(F(s_1) \cup F(s_2) \cup \ldots \cup F(S_A)\big), \\ (C(s_1) + C(s_2) + \cdots + C(s_A)) \leq C_{\text{зад}} \end{gathered} \tag{1.57}$$

и условию соответствия требованиям по эффективности защиты:

$$E(S) \geq E_{\text{треб}}, \tag{1.58}$$

где $E(S)$ – эффективность совокупности средств защиты S, $E_{\text{треб}}$ – требуемая эффективность системы защиты.

Определение 1.21. Оптимальным вариантом построения системы защиты будем называть такую совокупность средств защиты вида:

$$S = \{s_1; s_2; \ldots; s_A\}, \tag{1.59}$$

которая одновременно удовлетворяет условиям:

$$\begin{gathered} F_{\text{зад}} \subseteq (F(s_1) \cup F(s_2) \cup \ldots \cup F(S_A)), \\ (C(s_1) + C(s_2) + \cdots + C(s_A)) \leq C_{\text{зад}}, \\ E(S) \geq E_{\text{треб}} \end{gathered} \tag{1.60}$$

и оказывает минимальное влияние на производительность защищаемой системы:

$$\Delta\pi \to min, \Delta\pi = \pi - \pi_S, \quad (1.61)$$

где π_S – производительность защищаемой системы после введения в ее состав совокупности средств защиты S, π – производительность защищаемой системы до введения в ее состав совокупности средств защиты S.

Теоретико-методологический подход к формированию функциональных требований к системе защиты от компьютерных атак будет изложен во второй главе монографии, а теоретико-методологический подход к решению задачи выбора оптимального варианта построения системы защиты – в третьей.

2 Теоретико-методологический подход к формированию функциональных требований к системе защиты от компьютерных атак

2.1 Общая концепция формирования функциональных требований к системе защиты от компьютерных атак с использованием риск-ориентированного подхода

Основой для разработки и построения системы защиты от компьютерных атак для автоматизированных систем управления являются функциональные требования, которые формируются в соответствии с подходом к построению автоматизированных систем в защищенном исполнении [87, 97].

Оптимально сформированные и обоснованные функциональные требования к системе защиты от компьютерных атак позволят спроектировать и построить оптимальную систему защиты от компьютерных атак, которая с одной стороны, обеспечит необходимый уровень защиты, а с другой – будет потреблять минимальное количество вычислительных ресурсов защищаемой системы, что в свою очередь позволит минимизировать снижение эффективности защищаемой системы вследствие введения в ее состав системы защиты от компьютерных атак.

Задача формирования оптимального набора функциональных требований относится к задачам многокритериального принятия решения. Формальным описанием процесса выбора оптимального набора $F_{opt}(s_i)$ функциональных требований для i-го средства защиты s_i может служить модель оптимизации вида [139]:

$$F_{opt}(s_i) = opt\left(F_{full}(s_i)\right), \tag{2.1}$$

где $F_{full}(s_i)$ – множество всех возможных функциональных требований к i-му средству защиты s_i; opt – оператор оптимизации, определяющий правила выбора оптимального набора функциональных требований $F_{opt}(s_i)$.

Определение элементов множества всех возможных функциональных требований $F_{full}(s_i)$ для i-го средства защиты s_i возможно с использованием ряда нормативных документов (в частности [92, 129, 130, 131, 132, 133, 134, 135]), а также на основе

ГОСТ Р ИСО/МЭК 15408 [33, 34, 35] в соответствии с руководящими документами [117, 118, 122].

Одним из возможных путей формирования и обоснования оптимальных функциональных требований к системе защиты от компьютерных атак является применение подхода основанного на анализе и оценке рисков угроз безопасности информации в автоматизированной системе и угроз ее безопасного функционирования.

Данный подход базируется на следующих основных принципах [46]:

– принцип прогнозирования угроз безопасности в защищаемой АСУ;

– принцип достаточности мер защиты от компьютерных атак для некритичных компонентов и информационных ресурсов АСУ;

– принцип максимальной защиты критичных информационных ресурсов АСУ от компьютерных атак.

2.2 Исходные теоретические положения по формированию функциональных требований к системе защиты от компьютерных атак

Для формального описания предлагаемого подхода к формированию функциональных требований к системам защиты от компьютерных атак необходимо определить несколько положений.

Введем следующие обозначения: T – множество угроз безопасности АСУ; K – множество видов и способов реализации компьютерных атак; Q – множество элементов, входящих в состав АСУ, при этом (определение 1.1):

$$Q = A \cup S \cup C \cup H. \tag{2.2}$$

Положение 2.1. Имеется эффективный метод построения соответствия Φ_1 из множества T в множество Q, который определяется по следующему правилу:

$$(\forall t \in T)(\forall q \in Q)(t \Phi_1 q \Leftrightarrow \\ \Leftrightarrow \text{угроза } t \text{ представляет опасность для элемента } q). \tag{2.3}$$

Пусть $T^* = \{t_i^* | i = 1; 2; \dots; I\}$ – область определения соответствия Φ_1, то есть $T^* = Dom\Phi_1 \subseteq T$. Ограничение соответствия Φ_1 на подмножество T^* обозначим через Φ_1^*.

Соответствие Φ_1^* может быть представлено посредством графа $G(\Phi_1^*)$ (рисунок 2.1).

Это соответствие может быть также представлено в виде булевой матрицы rul_{T^*Q} размерности $I \times J$:

$$rul_{T^*Q} = \begin{pmatrix} \gamma_{11} & \gamma_{12} & \cdots & \gamma_{1J} \\ \gamma_{21} & \gamma_{22} & \cdots & \gamma_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_{I1} & \gamma_{I2} & \cdots & \gamma_{IJ} \end{pmatrix}, \quad (2.4)$$

где

$$\gamma_{ij} = \begin{cases} 1, \text{если угроза } t_i^* \text{представляет} \\ \quad \text{опасность для элемента } q_j \\ 0, \text{в противном случае} \end{cases}, i = \overline{1;I}, j = \overline{1;J}. \quad (2.5)$$

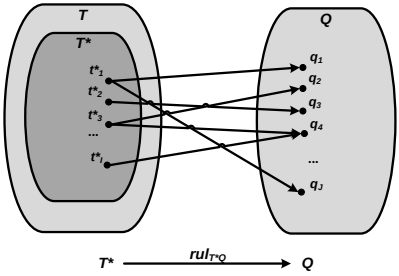


Рисунок 2.1 – Пример сопоставления элементов множества *T** элементам множества *Q*

Положение 2.2. Имеется эффективный метод построения соответствия Φ_2 из множества K в множество T, которое определяется по следующему правилу:

$$(\forall k \in K)(\forall t \in T)(k\Phi_2 t \Leftrightarrow$$
$$\Leftrightarrow \text{угроза } t \text{ может быть реализована посредством компьютерной атаки } k). \quad (2.6)$$

Пусть $K^* = \{k_l^* | l = 1; 2; \dots; L\}$ – область определения соответствия Φ_2. Тогда, в соответствии с положением 2.1, будем

иметь: $Im\Phi_2 = T^*$. Ограничение соответствия Φ_2 на подмножество K^* обозначим через Φ_2^*.

На рисунке 2.2 дается геометрическая реализация соответствия Φ_2^* посредством графа $G(\Phi_2^*)$.

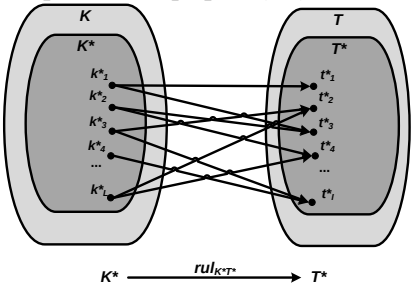


Рисунок 2.2 – Пример сопоставления элементов множества *K** элементам множества *T**

Матричное представление этого соответствия дается посредством матрицы $rul_{K^*T^*}$ размерности $L \times I$:

$$rul_{K^*T^*} = \begin{pmatrix} \tau_{11} & \tau_{12} & \cdots & \tau_{1I} \\ \tau_{21} & \tau_{22} & \cdots & \tau_{2I} \\ \vdots & \vdots & \ddots & \vdots \\ \tau_{L1} & \tau_{L2} & \cdots & \tau_{LI} \end{pmatrix}, \tag{2.7}$$

где

$$\gamma_{ij} = \begin{cases} 1, \text{если угроза } t_i^* \text{ может быть} \\ \quad \text{реализована атакой } k_l^* \\ 0, \text{в противном случае} \end{cases}, i = \overline{1;I}, l = \overline{1;L}. \tag{2.8}$$

Положение 2.3. Имеется эффективный метод построения соответствия Φ_3 из множества K в множество Q, которое определяется по следующему правилу:

$$(\forall k \in K)(\forall q \in Q)(k\Phi_3 q \Leftrightarrow \\ \Leftrightarrow \text{элемент } q \text{ является потенциальным объектом компьютерной атаки } k). \tag{2.9}$$

Наличие эффективного метода реализации этого положения является следствием существования соответствующих методов положений 2.1 и 2.2.

В частности, $Dom\Phi_3 = K^* \subseteq K$. Ограничение соответствия Φ_3 на подмножество K^* множества K обозначим через Φ_3^*. Графовая реализация соответствия Φ_3^* дана на рисунке 2.3.

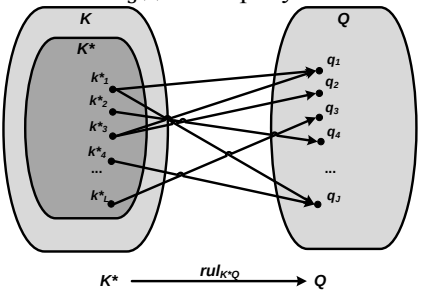


Рисунок 2.3 – Пример сопоставления элементов множества *K** элементам множества *Q*

Матричное представление этого соответствия дается этого соответствия дается посредством матрицы rul_{K^*Q} размерности $L \times J$:

$$rul_{K^*Q} = \begin{pmatrix} \mu_{11} & \mu_{12} & \cdots & \mu_{1J} \\ \mu_{21} & \mu_{22} & \cdots & \mu_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ \mu_{L1} & \mu_{L2} & \cdots & \mu_{LJ} \end{pmatrix}, \tag{2.10}$$

где

$$\mu_{ij} = \begin{cases} 1, \text{если элемент } q_j \text{ может} \\ \text{являться объектом атаки } k_l^*, i = \overline{1;I}, l = \overline{1;L}. \\ 0, \text{в противном случае} \end{cases} \tag{2.11}$$

Напомним, для дальнейшего, правило логического умножения булевых матриц $A = \|a_{ij}\|_{i=\overline{1;m}, j=\overline{1;n}}$ и $B = \|b_{ij}\|_{i=\overline{1;n}, j=\overline{1;t}}$. Предварительно заметим, что так как число столбцов матрицы A равно числу строк матрицы B, то традиционное умножение матриц является возможным и результатом этого произведения является числовая матрица размерности $m \times t$.

Для нахождения логического произведения $A \times B$ булевых матриц A и B эти матрицы умножаются по правилу умножения числовых матриц, но, при этом, при нахождении сумм произведений элементов строк матрицы A на соответствующие элементы столбцов матрицы B, арифметические операции сложения и умножения заменяются на их логические аналоги – конъюнкцию и дизъюнкцию, соответственно. То есть, обозначая элементы матрицы $A \times B$ через $\mu_{ij}, i = \overline{1;m}, j = \overline{1;t}$, будем иметь:

$$A \times B = \|\mu_{ij}\|, \tag{2.12}$$

где $\mu_{ij} = \bigvee_{k=1}^{n}(a_{ik} \wedge b_{kj}), \gamma_{ij}, i = \overline{1;m}, j = \overline{1;t}$.

Матрицы $rul_{K^*T^*}$ и rul_{T^*Q}, как формальные воплощения эффективности методов положений 2.1 и 2.2, соответственно, определяют матрицу rul_{K^*Q}, как формальный аналог эффективности метода положения 2.3, так как имеет место следующее утверждение.

Предложение 2.1. Матрица rul_{K^*Q} является логическим произведением матриц $rul_{K^*T^*}$ и rul_{T^*Q}, то есть:

$$rul_{K^*Q} = rul_{K^*T^*} \times rul_{T^*Q}, \tag{2.13}$$

Доказательство. Пусть $rul_{K^*T^*} \times rul_{T^*Q} = C = \|c_{ij}\|_{i=\overline{1;L}, j=\overline{1;I}}$. Покажем, что $\|c_{ij}\| = rul_{K^*Q}$. Так как $rul_{K^*Q} = \|\mu_{ij}\|_{i=\overline{1;L}, j=\overline{1;I}}$, то нужно доказать, что

$$c_{ij} = \mu_{ij}, \tag{2.14}$$

для любых $i \in \{1; 2; \dots; L\}; j \in \{1; 2; \dots; I\}$.

Действительно, для элемента c_{ij}, как элемента булевой матрицы, могут иметь место две возможности: а) $c_{ij} = 1$ и б) $c_{ij} = 0$. В связи с двойственностью этих возможностей, рассмотрим только первую из них.

а) По определению операции $\times$ – логического произведения, имеем:

$$c_{ij} = \bigvee_{r=1}^{I}(\tau_{ir} \wedge \gamma_{rj}). \tag{2.15}$$

Так как $c_{ij} = 1$, то хотя бы одно слагаемое логической суммы (2.15), согласно определению операции $\vee$ – дизъюнкции, должно быть равно 1. Пусть это будет слагаемое $\tau_{ir_0} \wedge \gamma_{r_0 j}$. Так как $\tau_{ir_0} \wedge \gamma_{r_0 j} = 1$, то в соответствии с определением операции $\wedge$ – конъюнкции, будем иметь: $\tau_{ir_0} = 1$ и $\gamma_{r_0 j} = 1$. Отсюда, получаем, основываясь на матричных представлениях для Φ_2^* и Φ_1^*, соответственно, что:

$$k_i^* \Phi_2^* t_{r_0}^* \tag{2.16}$$

и

$$t_{r_0}^* \Phi_1^* q_j^*. \tag{2.17}$$

Вербальными (словесными) формами утверждений (2.16) и (2.17) являются соответственно, высказывания:

– «компьютерная атака k_i^* реализует угрозу $t_{r_0}^*$»;

– «угроза $t_{r_0}^*$ представляет опасность для элемента q_j^* АСУ».

Непосредственным следствием этих высказываний является следующее высказывание:

– «потенциальным объектом компьютерной атаки k_i^* является элемент q_j^* АСУ», формальной версией которого является, согласно определению соответствия Φ_3^*, утверждение:

$$t_i^* \Phi_3^* q_j^*. \tag{2.18}$$

Так как $rul_{K^* Q}$ является матрицей соответствия Φ_3^*, то из (2.18) получаем, что $\mu_{ij} = 1$, что завершает доказательство равенства (2.14) в рассматриваемом случае а).

2.3 Оценка количественных характеристик рисков нарушения безопасности автоматизированной системы управления при воздействии компьютерных атак

Перейдем теперь к описанию технологий выявления количественных характеристик рисков нарушения безопасности АСУ при проведении на нее компьютерных атак.

С этой целью каждому элементу q_j множества Q ставится в соответствие весовой коэффициент w_j, характеризующий важность (критичность, с позиций безопасности АСУ) этого элемента $(j = \overline{1;J})$. В общем случае не исключается возможность того, что один и тот же весовой коэффициент может быть поставлен в соответствие различным элементам множества Q (смотри рисунок 2.4).

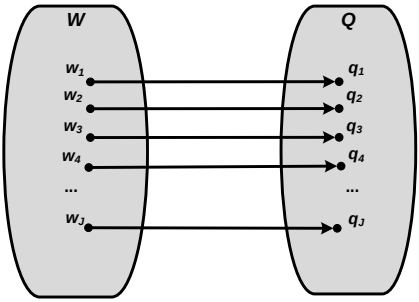


Рисунок 2.4 – Пример отображения множества *W* на множество *Q*

Весовой коэффициент w_j, характеризующий критичность j-го элемента множества Q определяется степенью возможных негативных последствий (ущерба) от реализации угроз безопасности в отношении этого элемента.

Для оценки критичности компонентов АСУ (элементов множества Q), предлагается использовать оценку степени возможных негативных последствий в случае реализации угрозы безопасности в отношении оцениваемого компонента АСУ по четырем уровням.

Критерии отнесения степени возможных негативных последствий к какому-либо из этих четырех уровней для угроз, направленных на нарушение штатного режима функционирования АСУ приведены в таблице 2.1. Предложенные критерии оценки степени возможных негативных последствий разработаны в соответствии с требованиями, изложенными в [26, 28, 113].

Критерии отнесения степени возможных негативных последствий к какому-либо из четырех уровней для угроз, направленных на нарушение безопасности информации различных категорий доступа, обрабатываемой и хранящейся в АСУ приведены в таблице 2.2.

Таблица 2.1 – Критерии определения степени ущерба для угроз, направленных на нарушение штатного режима функционирования АСУ

Степень критичности компонента	w_j	Характеристика критичности компонента
«высокая»	1	Воздействие на компонент АСУ может повлечь нарушение штатного режима функционирования АСУ, при этом возможны существенные негативные последствия (АСУ не сможет выполнять хотя бы одну из основных функций по управлению объектом).
«средняя»	0,7	Воздействие на компонент АСУ может повлечь нарушение штатного режима функционирования АСУ, при этом возможны умеренные негативные последствия (АСУ сможет выполнять основные функции по управлению объектом с существенной потерей эффективности).
«низкая»	0,4	Воздействие на компонент АСУ может повлечь нарушение штатного режима функционирования АСУ, при этом возможны незначительные негативные последствия (АСУ сможет выполнять основные функции по управлению объектом с незначительной потерей эффективности, АСУ не сможет выполнять хотя бы одну из второстепенных (вспомогательных) функций, выполнение всех функций АСУ в полном объеме возможно с привлечением дополнительных сил и средств).
«отсутствует»	0	Воздействие на ресурс АСУ не повлечет никаких негативных последствий.

Таблица 2.2 – Критерии определения степени ущерба для угроз, направленных на нарушение безопасности информационных ресурсов АСУ

Степень критичности компонента	w_j	Характеристика критичности компонента
«высокая»	1	Воздействие на компонент АСУ может повлечь нарушение безопасности информации ограниченного доступа, составляющей государственную тайну.
«средняя»	0,7	Воздействие на компонент АСУ может повлечь нарушение безопасности информации ограниченного доступа, составляющей служебную тайну, либо раскрытие особенностей построения АСУ.
«низкая»	0,4	Воздействие на компонент АСУ может повлечь нарушение безопасности информации, не составляющей государственную или служебную тайну, но относящейся к категории ограниченного доступа.
«отсутствует»	0	Воздействие на компонент АСУ не повлечет никаких негативных последствий.

Возможность проведения компьютерной атаки на какой-либо объект (компонент) АСУ характеризуется вероятностью проведения этой атаки в отношении атакуемого объекта (компонента) АСУ. Данная вероятность определяется

возможностями (потенциалом и мотивацией) нарушителя (субъекта, проводящего атаку), наличием или отсутствием уязвимостей в атакуемом объекте и степени их опасности, а также наличием угрозы, которая может быть реализована данной компьютерной атакой в отношении атакуемого объекта [36, 40, 47, 51, 54, 56]:

$$p = f\left(Pt_{\text{нар}}, M_{\text{нар}}, V_{\text{уязв}}, B_{\text{угр}}(k,q)\right), \tag{2.19}$$

где $Pt_{\text{НАР}}$ – потенциал нарушителя, зависящий от уровня его общей технической осведомленности, осведомленности об особенностях построения и функционирования атакуемой АСУ и его техническим оснащением (наличием или отсутствием технических средств, необходимых для проведения атаки) [40, 47, 50, 54]; $M_{\text{нар}}$ – мотивация нарушителя, $V_{\text{уязв}}$ – уровень опасности уязвимостей, имеющихся в атакуемом объекте (как правило определяется с помощью широко известной и применяемой методики CVSS [1, 45, 81, 95]); $B_{\text{угр}}$ – булева функция, определяющая наличие или отсутствие угрозы безопасности при проведении компьютерной атаки на атакуемый объект:

$$B_{\text{угр}}(k,q) = \begin{cases} 1, \text{если компьютерная атака } k \text{ несет угрозу} \\ \quad \text{в отношении атакуемого объекта } q \\ 0, \text{в противном случае} \end{cases}, \tag{2.20}$$

для любых $k \in K$ и $q \in Q$.

$B_{\text{угр}}$ может быть определено из матрицы rul_{K^*Q} (2.10), которая как раз и показывает наличие или отсутствие угрозы при проведении *i*-ой компьютерной атаки на *j*-й элемент АСУ. При этом от булевой матрицы rul_{K^*Q} можно перейти к матрице вероятностей проведения компьютерных атак в отношении АСУ в целом:

$$P_{K^*Q} = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1J} \\ p_{21} & p_{22} & \cdots & p_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ p_{L1} & p_{L2} & \cdots & p_{LJ} \end{pmatrix}, \tag{2.21}$$

где L – число видов и способов компьютерных атак (из множества K^*), J – число компонентов, входящих в состав АСУ, а элементы $(p_{ij}, l = \overline{1;L}, j = \overline{1;J})$ этой матрицы можно определить в

соответствии с выражением (2.19), с использованием различных методик, например, изложенной в [54].

Используя полученную матрицу вероятностей проведения компьютерных атак на АСУ и (весовые) коэффициенты важности (критичности) составных компонентов АСУ из множества W можно определить матрицу рисков нарушения безопасности АСУ при проведении на нее компьютерных атак [62]:

$$R = \begin{pmatrix} r_{11} & r_{12} & \cdots & r_{1J} \\ r_{21} & r_{22} & \cdots & r_{2J} \\ \vdots & \vdots & \ddots & \vdots \\ r_{L1} & r_{L2} & \cdots & r_{LJ} \end{pmatrix}, \quad (2.22)$$

где, как и ранее, L – число видов и способов компьютерных атак, J – число компонентов, входящих в состав АСУ, а элементы этой матрицы r_{lj} определяются следующим образом:

$$r_{ij} = p_{ij} \times w_j, \quad (2.23)$$

при $i = \overline{1;L}$, $j = \overline{1;J}$, w_j – коэффициент характеризующий важность (критичность) j-го компонента из состава АСУ. В данном случае нужно понимать, что w_j – некоторое неотрицательное число (таблица 2.1, таблица 2.2), а «×» – обычное произведение вероятности p_{ij} (т. е. число) на w_j или математическое ожидание риска r_{ij}.

Таким образом, элемент матрицы рисков r_{lj} характеризует риск нарушения безопасности j-го компонента АСУ вследствие реализации угрозы безопасности l-ой компьютерной атакой по этому компоненту, а под риском нарушения безопасности посредством компьютерной атаки в данном случае понимается сочетание вероятности реализации той или иной угрозы в отношении того или иного компонента АСУ с помощью той или иной компьютерной атаки и степени тяжести последствий реализации этой угрозы для атакуемой АСУ [4, 12, 20].

2.4 Формирование функциональных требований к системе защиты от компьютерных атак

Полученная в пункте 2.3 матрица рисков нарушения безопасности АСУ (2.22) является основой для формирования

функциональных требований к системе защиты от компьютерных атак.

Для описания этих требований сформулируем, в дополнение к положениям 2.1 – 2.3, еще ряд положений.

Положение 2.4. Будем предполагать, что для каждой компьютерной атаки из множества K^* можно эффективным способом определить совокупность средств защиты, которая будет способна полностью нейтрализовать данную компьютерную атаку. Т. е. что каждому элементу множества K^* можно поставить в соответствие определенную совокупность средств защиты S_i^* ($i = \overline{1;L}$, где L, как и ранее, число видов и способов компьютерных атак), которая будет являться подмножеством общего множества S, элементы которого представляют собой отдельные составляющие системы защиты от компьютерных атак в целом (рисунок 2.5). На этом рисунке, с целью обеспечения наибольшей наглядности, различные подмножества $S_{l_1}^*$ и $S_{l_2}^*$, $1 \le l_1 < l_2 \le L$, изображены, как непересекающиеся. Тем не менее, в общем случае, их пересечения и даже совпадения – не исключаются.

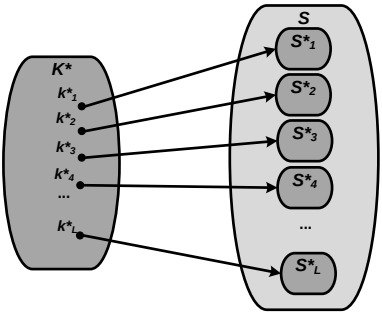


Рисунок 2.5 – Пример сопоставления каждой компьютерной атаке совокупности средств защиты

Для дальнейшего, через S обозначим множество $\bigcup_{l=1}^{L} S_l^*$. Будем полагать, что $S^* = \{s_1^*; s_2^*; \dots; s_R^*\}$. В общем случае S^* может не совпадать с S, т.е. $S^* \subset S$.

Каждое множество S_i^*, которое входит в виде подмножества в множество S, включает в себя определенное число средств защиты (число элементов множеств $S_1^*, S_2^*, \dots, S_i^*, \dots, S_L^*$ зависит от видов и способов компьютерных атак, для нейтрализации которых они

предназначены). Распределение средств защиты по соответствующим совокупностям задается матрицей защиты:

$$R = \begin{pmatrix} h_{11} & h_{12} & \cdots & h_{1R} \\ h_{21} & h_{22} & \cdots & h_{2R} \\ \vdots & \vdots & \ddots & \vdots \\ h_{L1} & h_{L2} & \cdots & h_{LR} \end{pmatrix}, \quad (2.24)$$

где L – число видов и способов компьютерных атак, R – число средств защиты множества S^*, а элементы этой матрицы h_{lr} определяются следующим образом:

$$h_{lr} = \begin{cases} 1, \text{если средство защиты } s_r^* \text{ необходимо для} \\ \quad \text{нейтрализации компьютерной атаки } k_l^* \\ 0, \text{в противном случае} \end{cases}. \quad (2.25)$$

Пример 2.1. Для $L = 5$ (число видов и способов компьютерных атак) и $R = 6$ (число средств защиты) зададим распределение средств защиты следующим образом (таблица 2.3):

Таблица 2.3 – Пример распределения средств защиты

Средства защиты / Виды и способы компьютерных атак	s*1	s*2	s*3	s*4	s*5	s*6
k1	1	1	0	1	0	0
k2	1	0	1	0	1	0
k3	0	1	0	0	0	1
k4	1	0	0	0	0	1
k5	0	1	1	1	0	1

То есть, применительно к этому примеру, будем иметь:

$$S^* = \{s_1^*; s_2^*; s_3^*; s_4^*; s_5^*; s_6^*\}. \quad (2.26)$$

$$S_1^* = \{s_1^*; s_2^*; s_4^*\}; S_2^* = \{s_1^*; s_3^*; s_5^*\}; S_3^* = \{s_2^*; s_6^*\}; \\ S_4^* = \{s_1^*; s_6^*\}; S_5^* = \{s_2^*; s_3^*; s_4^*; s_6^*\}. \quad (2.27)$$

Положение 2.5. Будем полагать, что каждое средство защиты s_r^* $(r = \overline{1;R})$ имеет определенный набор функций X_r, характеризующих степень обеспечения ими защиты:

$$X_r = \{x_{r1}; x_{r2}; \dots; x_{rN}\}, \quad (2.28)$$

где N – количество функций этого средства защиты. При этом все множество функций X_r можно разделить на k подмножеств таким образом, что:

$$X_r = \{X_{r1} \cup X_{r2} \cup \ldots \cup X_{rN}\}, \quad (2.29)$$

при этом $X_{r1} \subset X_{r2}$; $X_{r2} \subset X_{r3}$;…; $X_{rk-1} \subset X_{rk}$ (рисунок 2.6).

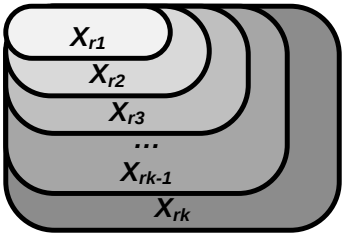


Рисунок 2.6 – Деление множества X_r на подмножества

Через s_{rt}^* обозначим средство защиты s_r^*, совокупность X_r – функций которого ограничена до подсовокупности X_{rt}, $t = 1; 2; \ldots; k$.

Тогда средство защиты s_{r1}^*, как средство, имеющее набор функций X_{r1} будет обеспечивать минимальную эффективность защиты, однако при этом будет потреблять минимальное количество ресурсов для своего функционирования, средство защиты s_{rk}^*, как средство, имеющее набор функций X_{rk}, будет обеспечивать максимальную эффективность защиты, потребляя при этом максимальное количество ресурсов для своего функционирования, а средства защиты $s_{r2}^*; s_{r3}^*; \ldots; s_{rk-1}^*$ с функциями $X_{r2}, X_{r3}, \ldots, X_{rk-1}$ будут обеспечивать промежуточные (между минимальным и максимальным) уровни защиты.

Полагая, что эффективность средств защиты определяется числом реализуемых функций и, обозначая через g_t число реализуемых функций средства защиты s_{rt}^*, а через z_t – потребляемые этим средством ресурсы, будем иметь:

$$g_1 < g_2 < \ldots < g_k \quad (2.30)$$

и

$$z_1 < z_2 < \ldots < z_k. \quad (2.31)$$

Положение 2.6. Будем считать, что каждому элементу x_r множества $X_r = \{x_{ri} | i = \overline{1;N}\}$ функций каждого средства защиты можно поставить в соответствие один из элементов f множества функциональных требований F. Будем полагать, при этом, что требование f_i будет задавать условие наделения этого средства защиты функцией x_{ri}, $i = \overline{1;N}$ (рисунок 2.7).

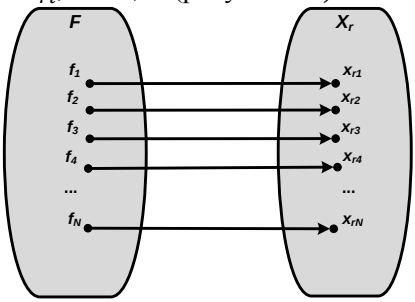


Рисунок 2.7 – Пример сопоставления элементов множества функциональных требований элементам множества функций средства защиты

Положение 2.7. Для каждого оценочного значения r_{lj} риска из матрицы риска (2.22) можно определить свое подмножество функций $X_{rl_t} \in \{X_{r1}; X_{r2}; \dots X_{rk}\}$, $t = \overline{1;k}$ из множества X_r следующим образом: минимальному значению риска соответствует множество функциц X_{r1}, максимальному значению риска соответствует множество функций X_{rk}, промежуточным значениям риска соответствуют промежуточные множества функций $X_{r2}, X_{r3}, \dots, X_{rk-1}$ по возрастанию. При этом t будет являться уровнем реализации функций каждого отдельного средства. Т. е. чем больше функций входит в подмножество X_{rl_t}, тем выше уровень реализации функций.

Принцип формирования функциональных требований к системе защиты АСУ от компьютерных атак заключается в выборе необходимого набора функций X_r (и соответствующих этим свойствам функциональных требований F) для каждого средства защиты s, входящего в совокупности средств защиты $S_1^*, S_2^*, \dots, S_R^*$ из которых в свою очередь строится система защиты S от компьютерных атак.

Правило выбора необходимого набора функций основано на положении 2.7. Для начала определяется количество уровней риска

(наиболее приемлемым является четыре уровня риска: «отсутствует», «низкий», «средний», «высокий» [54]), и определяются граничные значения риска для каждого уровня.

После чего формируют множества свойств $X_{r1}, X_{r1}, \dots, X_{rk}$ для каждого средства (где k – число уровней значений риска) исходя из положения 2.7. Далее, используя матрицу распределения средств защиты (2.24) для каждой компьютерной атаки из множества K^* определяют необходимые совокупности средств защиты, а используя матрицу риска (2.22) определяют необходимые наборы функций для каждой совокупности средств защиты, формируя при этом матрицу M уровней реализации функции средств защиты:

$$M = \begin{pmatrix} m_{11} & m_{12} & \cdots & m_{1R} \\ m_{21} & m_{22} & \cdots & m_{2R} \\ \vdots & \vdots & \ddots & \vdots \\ m_{L1} & m_{L2} & \cdots & m_{LR} \end{pmatrix}, \quad (2.32)$$

где L– число видов и способов компьютерных атак, R – число средств защиты, а элементы m_{ij}, $i = \overline{1;L}$, $j = \overline{1;R}$ этой матрицы определяются числовыми значениями уровней реализации функций для каждого средства.

Пример 2.2. Исходя из матрицы распределения средств защиты (таблица 2.1) и следующих уровней риска для компьютерных атак (по методике, изложенной в [54]): k_1 – «высокий», k_2 – «низкий», k_3 – «отсутствует», k_4 – «средний», k_5 – «высокий» определим матрицу уровней реализации функций средств защиты следующим образом (таблица 2.4):

Таблица 2.4 – Пример матрицы уровней реализации функций средств защиты

Средства защиты Виды, способы компьютерных атак и их уровень риска	s_1^*	s_2^*	s_3^*	s_4^*	s_5^*	s_6^*
k1 «высокий»	4	4	0	4	0	0
k2 «низкий»	2	0	2	0	2	0
k3 «отсутствует»	0	1	0	0	0	1
k4 «средний»	3	0	0	0	0	3
k5 «средний»	0	3	3	3	0	3

При этом использовалось соответствие уровней риска компьютерных атак уровням реализации свойств средств защиты определенное в таблице 2.5.

Таким образом, совокупность S^* будет представлять собой объединение следующих средств защиты:

$$S^* = \{\{s_1^*(4); s_2^*(4); s_4^*(4)\}; \{s_1^*(2); s_3^*(2); s_5^*(2)\}; \{s_2^*(1); s_6^*(1)\}; \{s_1^*(3); s_6^*(3)\}; \{s_2^*(3); s_3^*(3); s_4^*(3); s_6^*(3)\}\}. \quad (2.33)$$

где $s_i^*(k)$ следует понимать как i-е средство с k-м уровнем реализации свойств.

Таблица 2.5 – Соответствие уровней риска компьютерных атак уровням реализации функций средств защиты

Уровень риска	Уровень реализации функций средств защиты
«высокий»	4
«средний»	3
«низкий»	3
«отсутствует»	1

Следует отметить, что сформированное таким образом множество S^* (которое представляет собой по сути вариант построения системы защиты) обладает избыточностью, от которой можно избавиться, применив следующие правила:

Правило «сокращения» (R_{RED}) – если множество S^* содержит несколько одинаковых средств защиты с одинаковым уровнем реализации функций, то количество этих средств сокращается до одного.

Правило «поглощения» (R_{ABS}) – если множество S^* содержит несколько одинаковых средств защиты с разными уровнями реализации функций, то все средства с уровнем реализации функций меньшим максимального поглощаются средством с максимальным уровнем реализации (т. е. во множестве S^* остается только функция с максимальным уровнем реализации).

Данные правила реализуются следующим образом:

– в каждом столбце матрицы реализации функций производится поиск максимального элемента;

– номер столбца будет являться номером средства защиты, которое будет включено в систему защиты (если все элементы текущего столбца равны нулю, то средство текущего номера в состав системы защиты не включается);

– уровнем реализации функции для средства защиты будет являться максимальное значение текущего столбца матрицы.

Формально это можно записать следующим образом:

$$S^* \xrightarrow{R_{RED};R_{ABS}} \hat{S} \tag{2.34}$$

$$\hat{S} = \{s_1^*(max(m_{11}; m_{21}; \dots; m_{L1})); \\ s_2^*(max(m_{12}; m_{22}; \dots; m_{L2})); \dots; \\ s_R^*(max(m_{1R}; m_{2R}; \dots; m_{LR}))\} \tag{2.35}$$

где m_{ij} – элемент матрицы уровней реализации функций M.

Пример 2.3. Исходя из матрицы уровней реализации функций из примера 2.2 (таблица 2.4) и используя выражение (2.35) сформируем множество $\hat{S}$ следующим образом (рисунок 2.8):

$$\hat{S} = \{s_1^*(4); s_2^*(4); s_3^*(3); s_4^*(4); s_5^*(2); s_6^*(3)\}. \tag{2.36}$$

Средства защиты Виды, способы компьютерных атак и их уровень риска	s^*_1	s^*_2	s^*_3	s^*_4	s^*_5	s^*_6
k_1 «высокий»	4	4	0	4	0	0
k_2 «низкий»	2	0	2	0	2	0
k_3 «отсутствует»	0	1	0	0	0	1
k_4 «средний»	3	0	0	0	0	3
k_5 «средний»	0	3	3	3	0	3

Рисунок 2.8 – Пример сопоставления множеств функций X_k значениям риска

После формирования множества средств защиты $\hat{S}$, используя положение 2.6, можно перейти от множества функций для каждого средства защиты к множеству функциональных требований, необходимых для реализации этих свойств.

Таким образом, формирование оптимальных требований к системе защиты от компьютерных атак будет заключаться:

– в выборе необходимых совокупностей средств защиты $\{S^*_1, S^*_2, \dots, S^*_L\}$ для каждой компьютерной атаки;

– в выборе нужного набора функций для каждого средства, входящего в совокупности средств защиты;

– в приведении полученного множества средств защиты S^* к рациональной форме $\hat{S}$ с использованием правила «сокращения» и правила «поглощения»;

– в формировании функциональных требований по обеспечению нужного набора функций для каждого средства защиты, входящего в совокупности средств защиты.

Пример функциональных требований к средствам резервного копирования информации для четырех уровней реализации приведен в приложении В.

Применение предложенного подхода обеспечивает возможность формирования оптимальных функциональных требований, позволяющих спроектировать и построить оптимальную систему защиты, которая с одной стороны, обеспечит необходимый уровень защиты, а с другой – будет потреблять минимальное количество вычислительных ресурсов защищаемой АСУ, что в свою очередь позволит минимизировать фактор снижения эффективности защищаемой системы вследствие введения в ее состав системы защиты от компьютерных атак.

3 Теоретико-методологический подход к выбору оптимального варианта построения системы защиты от компьютерных атак

3.1 Общая концепция выбора оптимального варианта построения системы защиты от компьютерных атак

Исходя из многоуровневого построения автоматизированных систем управления (рисунок 1.2), система защиты от компьютерных атак должна быть построена в виде совокупности отдельных систем защиты для каждого уровня построения автоматизированной системы управления.

Таким образом, система защиты S от компьютерных атак в общем виде представляет собой множество:

$$S = \{S_1, S_2, \dots, S_N\}, \tag{3.1}$$

где N – число уровней автоматизированной системы, $S_i = \{s_{i1}, s_{i2}, \dots, s_{iH_i}\}$ – система защиты i-го уровня защищаемой автоматизированной системы, $i = \overline{1;N}$. Числа $H_1, H_2, \dots, H_N$ – элементов во множествах $S_1, S_2, \dots, S_N$, соответственно, в общем случае могут быть различными.

Система защиты S_i для каждого уровня может быть сформировано из множества $S^* = \{s_1, s_2, \dots, s_{M^*}\}$ всех имеющихся в наличии средств защиты, где M^* – число этих средств.

Таким образом:

$$S_i \subseteq S^*, i = \overline{1;N}. \tag{3.2}$$

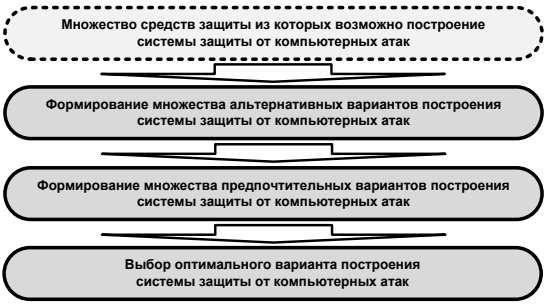


Рисунок 3.1 – Этапы построения оптимального варианта системы защиты от компьютерных атак

Формирование оптимального варианта построения системы защиты заключается в многоэтапном выборе оптимального варианта из всех возможных вариантов построения системы защиты (рисунок 3.1).

3.2 Сущность и содержание этапов выбора оптимального варианта построения системы защиты от компьютерных атак

3.2.1 Формирование множества альтернативных вариантов построения системы защиты от компьютерных атак

Формирование множества альтернативных вариантов построения системы защиты от компьютерных атак включает в себя три подэтапа (рисунок 3.2) [53].

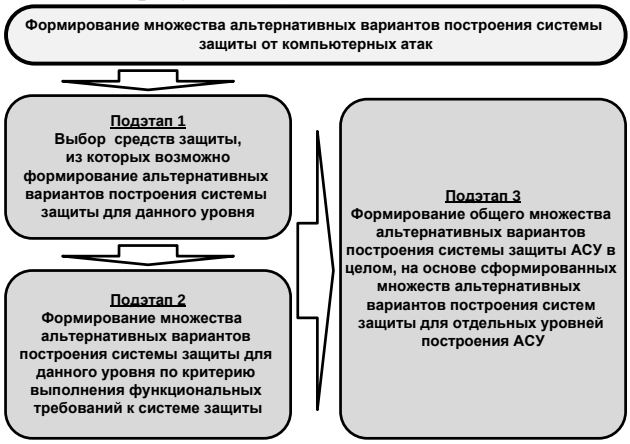


Рисунок 3.2 – Подэтапы формирования множества альтернативных вариантов построения системы защиты от компьютерных атак

1 подэтап (выполняется для каждого уровня защищаемой системы): Выбор из множества S^* таких средств защиты, из которых возможно формирование альтернативных вариантов построения системы защиты для данного (i-го) уровня, т. е. формирование множества ${S_i}^{**}$ средств защиты таким образом, что:

$$\left(\forall s_{ij} \in {S_i}^{**}\right)\left(\left(F\left(s_{ij}\right) \cap F_{\text{зад}}^{(i)}\right) \neq \emptyset\right), j = \overline{1; M_i^{**}}, i = \overline{1; N}, \qquad (3.3)$$

где $F(s_{ij})$ – множество функциональных требований реализуемых j-м средством защиты для i-го уровня, $F_{зад}^{(i)}$ – множество заданных функциональных требований для системы защиты данного (i-го) уровня ($i = \overline{1;N}$), $M^{**}{}_i$ – число элементов множества средств защиты, из которых возможно формирование альтернативных вариантов построения системы защиты для данного (i-го) уровня.

2 подэтап (выполняется для каждого уровня защищаемой системы): Формирование множества $X_{\text{уровн}}^{(i)}$ ($i = \overline{1;N}$) альтернативных вариантов построения системы защиты для данного (i-го) уровня по критерию выполнения функциональных требований к системе защиты:

$$X_{\text{уровн}}^{(i)} = \left\{x_{ij}^0 | F_{\text{зад}}^{(i)} \subseteq F\left(x_{ij}^0\right)\right\}, j = \overline{1;J_i}, i = \overline{1;N}, \tag{3.4}$$

где x_{ij}^0 – j-й вариант построения системы защиты для данного (i-го) уровня, удовлетворяющий множеству функциональных требований $F_{зад}^{(i)}$ данного (i-го) уровня, $F\left(x_{ij}^0\right)$ – множество функциональных требований, реализуемых j-м вариантом построения системы защиты, J_i – число вариантов построения системы защиты для данного (i-го) уровня.

Каждый (j-й) вариант x_{ij}^0 построения системы защиты для i-го уровня представляет собой совокупность средств защиты и формируется из отдельных средств защиты из множества $S_i{}^{**}$.

Информацию о результатах реализации функциональных требований отдельными средствами защиты для данного (i-го) уровня можно представить в виде матрицы реализации требований:

$$RF_i = \begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1C_i} \\ v_{21} & v_{22} & \cdots & v_{2C_i} \\ \cdots & \cdots & \ddots & \cdots \\ v_{M_i^{**}1} & v_{M_i^{**}2} & \cdots & v_{M_i^{**}C_i} \end{pmatrix}. \tag{3.5}$$

Элементы данной матрицы формируются с учетом следующего условия:

$$v_{kj} = \begin{cases} 1, & \text{если } k\text{-е средство реализует } j\text{-е требование} \\ 0, & \text{в противном случае} \end{cases}, \tag{3.6}$$

где $k = \overline{1; M_i^{**}}$, $j = \overline{1; C_i}$, M_i^{**} – число элементов множества средств защиты, из которых возможно формирование альтернативных вариантов построения системы защиты для данного (i-го) уровня, C_i – число элементов множества функциональных требований $F_{зад}^{(i)}$ для данного (i-го) уровня построения АСУ.

Для формирования каждого альтернативного варианта построения системы защиты для i-го уровня используются выборки из отдельных элементов множества $S_i^{**} = \{s_1; s_2; \dots; s_{M_i^{**}}\}$ (без повторений), т. е. подмножество этого исходного множества.

Так как число элементов множества S_i^{**} равно M_i^{**}, то число всех его подмножеств равно $2^{M_i^{**}}$, а так как в это число входит и пустое подмножество, которое никакого варианта защиты не дает, то общее число возможных вариантов будет определяться следующим образом:

$$N = 2^{M_i^{**}} - 1. \tag{3.7}$$

Таким образом, формирование множества альтернативных вариантов заключается в выборе всех подмножеств множества S_i^{**}, удовлетворяющих функциональным требованиям.

Общий подход в последовательном индуцировании всех альтернативных вариантов построения системы защиты для i-го уровня автоматизированной системы управления можно представить в виде многошаговой процедуры (в которой число шагов равно числу функциональных требований для i-го уровня) C_i следующим образом:

Шаг 1: Функциональное требование $f_1^{(i)}$ для i-го уровня автоматизированной системы управления может быть выполнено за счет включения в вариант построения тех элементов $s_{k_n^1}^{(i)}$ из множества S_i^{**}, которым соответствуют элементы первого столбца матрицы реализации требований, равные единице. Пусть $v_{k_1^1 1}^{(i)}; v_{k_2^1 1}^{(i)}; \dots; v_{k_{n_1}^1 1}^{(i)}$ – все такие элементы (где $k_1^1; k_2^1; \dots; k_{n_1}^1$ – номера элементов первого столбца матрицы реализации требований, равных единице; n_1 – число элементов первого столбца матрицы реализации требований, равных единице). Тогда требование $f_1^{(i)}$может быть реализовано или за счет включения в

вариант построения системы защиты средства $s_{k_1^1}^{(i)}$, или за счет включения в вариант построения системы защиты средства $s_{k_2^1}^{(i)}$, …, или за счет включения в вариант построения системы защиты средства $s_{k_{n_1}^1}^{(i)}$, что приводит к логической сумме:

$$\rho_1^{(i)} = s_{k_1^1}^{(i)} \vee s_{k_2^1}^{(i)} \vee \ldots \vee s_{k_{n_1}^1}^{(i)}. \quad (3.8)$$

Шаг 2. Аналогичным образом, функциональное требование $f_2^{(i)}$ для i-го уровня автоматизированной системы управления может быть выполнено за счет включения в вариант построения тех элементов $s_{k_n^2}^{(i)}$ из множества S_i^{**}, которым соответствуют элементы второго столбца матрицы реализации требований, равные единице. Пусть $v_{k_1^2 2}^{(i)}; v_{k_2^2 2}^{(i)}; \ldots; v_{k_{n_2}^2 2}^{(i)}$ – все такие элементы (где $k_1^2;\ k_2^2; \ldots; k_{n_2}^2$ – номера элементов второго столбца матрицы реализации требований, равных единице; n_2 – число элементов второго столбца матрицы реализации требований, равных единице). Тем самым, получаем вторую логическую сумму:

$$\rho_2^{(i)} = s_{k_1^2}^{(i)} \vee s_{k_2^2}^{(i)} \vee \ldots \vee s_{k_{n_2}^2}^{(i)}. \quad (3.9)$$

Шаг 3. По аналогии с шагом 1 и шагом 2, получаем логическую сумму:

$$\rho_3^{(i)} = s_{k_1^3}^{(i)} \vee s_{k_2^3}^{(i)} \vee \ldots \vee s_{k_{n_3}^3}^{(i)}. \quad (3.10)$$

Далее производится необходимое число шагов для каждого столбца матрицы реализации требований. Завершается процесс шагом с номером C_i.

Шаг C_i. Необходимость выполнения функционального требования $f_{C_i}^{(i)}$ приводит к получению, на основе C_i-го столбца матрицы реализации требований, логической суммы:

$$\rho_{C_i}^{(i)} = s_{k_1^{C_i}}^{(i)} \vee s_{k_2^{C_i}}^{(i)} \vee \ldots \vee s_{k_{n_{C_i}}^{C_i}}^{(i)}. \quad (3.11)$$

Определим булеву функцию P_0, как конъюнктивную нормальную форму (К.Н.Ф.) вида:

$$P_0 = \left(s_{k_1^1}^{(i)} \vee s_{k_2^1}^{(i)} \vee \ldots \vee s_{k_{n_1}^1}^{(i)}\right) \wedge \left(s_{k_1^2}^{(i)} \vee s_{k_2^2}^{(i)} \vee \ldots \vee s_{k_{n_2}^2}^{(i)}\right) \wedge \ldots \wedge \wedge \left(s_{k_1^{C_i}}^{(i)} \vee s_{k_2^{C_i}}^{(i)} \vee \ldots \vee s_{k_{n_{C_i}}^{C_i}}^{(i)}\right). \quad (3.12)$$

Используя законы логики, преобразуем ее к дизъюнктивной нормальной форме (Д.Н.Ф):

$$P_0 = \bigvee_{1 \le j_1 \le n_1;\ 1 \le j_2 \le n_2; \ldots;\ 1 \le j_l \le n_{C_i}} \left(s_{j_1}^{(i)} \wedge s_{j_2}^{(i)} \wedge \ldots \wedge s_{j_l}^{(i)}\right). \quad (3.13)$$

Каждое слагаемое полученной Д.Н.Ф. и будет представлять собой альтернативный вариант построения системы защиты для i-го уровня защищаемой автоматизированной системы управления.

Таким образом, сформированные множества альтернативных вариантов построения системы защиты для каждого уровня будут иметь вид:

$$\begin{gathered} X_{\text{уровн}}^{(1)} = \left\{x_{11}^0; x_{12}^0; \ldots; x_{1J_1}^0\right\} \\ X_{\text{уровн}}^{(2)} = \left\{x_{21}^0; x_{22}^0; \ldots; x_{2J_2}^0\right\} \\ \ldots \\ X_{\text{уровн}}^{(N)} = \left\{x_{N1}^0; x_{N2}^0; \ldots; x_{NJ_N}^0\right\} \end{gathered} . \quad (3.14)$$

3 подэтап: Формирование общего множества X альтернативных вариантов построения системы защиты АСУ в целом, на основе сформированных множеств $X_{\text{уровн}}^{(i)}$ вариантов построения систем защиты для отдельных уровней, $(i = \overline{1;N})$.

Для получения одного из альтернативных вариантов построения системы защиты выбираем из $X_{\text{уровн}}^{(1)}$ любой из элементов, например $x_{1k_1}^0$; из $X_{\text{уровн}}^{(2)}$ – элемент $x_{2k_2}^0$; …; из $X_{\text{уровн}}^{(N)}$ – элемент $x_{Nk_N}^0$; т. е. и $x_{1k_1}^0$ и $x_{2k_2}^0$ и … и $x_{Nk_N}^0$, что приводит к конъюнкции вида:

$$(x_{1k_1}^0 \wedge x_{2k_2}^0 \wedge \ldots \wedge x_{Nk_N}^0). \quad (3.15)$$

Для единообразного получения всех подобных конъюнкций, а следовательно, и всех общих вариантов построения систем защиты рассмотрим булеву функцию:

$$P_1 = \left(x_{11}^0 \vee x_{12}^0 \vee \ldots \vee x_{1J_1}^0\right) \wedge \left(x_{21}^0 \vee x_{22}^0 \vee \ldots \vee x_{2J_2}^0\right) \wedge \ldots \wedge \\ \wedge \left(x_{N1}^0 \vee x_{N2}^0 \vee \ldots \vee x_{NJ_N}^0\right), \tag{3.16}$$

т. е. P_1 является К.Н.Ф. – логическим произведением логических сумм. Используя законы логики, преобразуем ее к Д.Н.Ф.

Тогда получим:

$$P_1 = \bigvee_{1 \le k_1 \le J_1;\ 1 \le k_2 \le J_2; \ldots;\ 1 \le k_N \le J_N} \left(x_{1k_1}^0 \wedge x_{2k_2}^0 \wedge \ldots \wedge x_{Nk_N}^0\right). \tag{3.17}$$

Число «слагаемых» в этой логической сумме будет равно:

$$T = J_1 \cdot J_2 \cdot \ldots \cdot J_N, \tag{3.18}$$

т. е и число альтернативных вариантов построения системы защиты от компьютерных атак для АСУ будет равно T, а множество альтернативных вариантов построения системы защиты будет иметь вид:

$$X = \{x_1; x_2; \ldots; x_T\}. \tag{3.19}$$

Пример 3.1. Пусть, для $N = 3$, $J_1 = 4$, $J_2 = 3$, $J_3 = 2$, множество альтернативных вариантов построения системы защиты для каждого уровня будут иметь вид:

$$X_{\text{уровн}}^{(1)} = \{x_{11}^0; x_{12}^0; x_{13}^0;\ x_{14}^0\} \\ X_{\text{уровн}}^{(2)} = \{x_{21}^0; x_{22}^0; x_{23}^0\} \\ X_{\text{уровн}}^{(3)} = \{x_{31}^0; x_{32}^0\} \tag{3.20}$$

Тогда функция P_1 в виде К.Н.Ф будет иметь следующий вид:

$$P_1 = (x_{11}^0 \vee x_{12}^0 \vee x_{13}^0 \vee\ x_{11}^0) \wedge (x_{21}^0 \vee x_{22}^0 \vee x_{23}^0) \wedge \\ \wedge (x_{31}^0 \vee x_{32}^0). \tag{3.21}$$

Перейдя от К.Н.Ф к Д.Н.Ф получим:

$$
\begin{aligned}
P_1 = {} & (x_{11}^0 \wedge x_{21}^0 \wedge x_{31}^0) \vee (x_{11}^0 \wedge x_{21}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{11}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{11}^0 \wedge x_{22}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{11}^0 \wedge x_{23}^0 \wedge x_{31}^0) \vee (x_{11}^0 \wedge x_{23}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{12}^0 \wedge x_{21}^0 \wedge x_{31}^0) \vee (x_{12}^0 \wedge x_{21}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{12}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{12}^0 \wedge x_{22}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{12}^0 \wedge x_{23}^0 \wedge x_{31}^0) \vee (x_{12}^0 \wedge x_{23}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{13}^0 \wedge x_{21}^0 \wedge x_{31}^0) \vee (x_{13}^0 \wedge x_{21}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{13}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{13}^0 \wedge x_{22}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{13}^0 \wedge x_{23}^0 \wedge x_{31}^0) \vee (x_{13}^0 \wedge x_{23}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{14}^0 \wedge x_{21}^0 \wedge x_{31}^0) \vee (x_{14}^0 \wedge x_{21}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{14}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{14}^0 \wedge x_{22}^0 \wedge x_{32}^0) \vee \\
& \vee (x_{14}^0 \wedge x_{23}^0 \wedge x_{31}^0) \vee (x_{14}^0 \wedge x_{23}^0 \wedge x_{32}^0).
\end{aligned}
\tag{3.22}
$$

Таким образом, множество X альтернативных вариантов построения системы защиты, в данном случае, будет выглядеть следующим образом:

$$
\begin{aligned}
X = \{ & \{x_{11}^0; x_{21}^0; x_{31}^0\}; \{x_{11}^0; x_{21}^0; x_{32}^0\}; \{x_{11}^0; x_{22}^0; x_{31}^0\}; \\
& \{x_{11}^0; x_{22}^0; x_{32}^0\}; \{x_{11}^0; x_{23}^0; x_{31}^0\}; \{x_{11}^0; x_{23}^0; x_{32}^0\}; \\
& \{x_{12}^0; x_{21}^0; x_{31}^0\}; \{x_{12}^0; x_{21}^0; x_{32}^0\}; \{x_{12}^0; x_{22}^0; x_{31}^0\}; \\
& \{x_{12}^0; x_{22}^0; x_{32}^0\}; \{x_{12}^0; x_{23}^0; x_{31}^0\}; \{x_{12}^0; x_{23}^0; x_{32}^0\}; \\
& \{x_{13}^0; x_{21}^0; x_{31}^0\}; \{x_{13}^0; x_{21}^0; x_{32}^0\}; \{x_{13}^0; x_{22}^0; x_{31}^0\}; \\
& \{x_{13}^0; x_{22}^0; x_{32}^0\}; \{x_{13}^0; x_{23}^0; x_{31}^0\}; \{x_{13}^0; x_{23}^0; x_{32}^0\}; \\
& \{x_{14}^0; x_{21}^0; x_{31}^0\}; \{x_{14}^0; x_{21}^0; x_{32}^0\}; \{x_{14}^0; x_{22}^0; x_{31}^0\}; \\
& \{x_{14}^0; x_{22}^0; x_{32}^0\}; \{x_{14}^0; x_{23}^0; x_{31}^0\}; \{x_{14}^0; x_{23}^0; x_{32}^0\}\}.
\end{aligned}
\tag{3.23}
$$

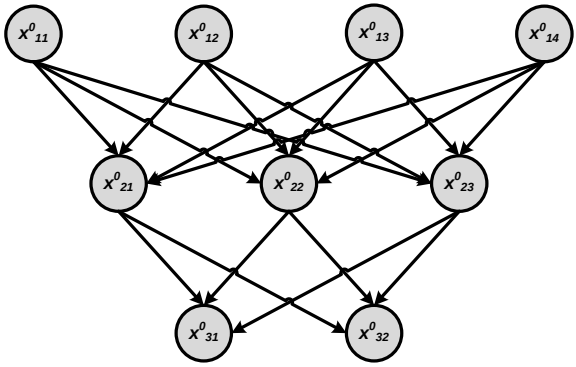


Рисунок 3.3 – Пример построения множества X альтернативных вариантов

Множество вершин каждого простого максимального пути этого графа дает один из альтернативных вариантов системы защиты.

3.2.2 Формирование допустимых по стоимости вариантов построения системы защиты от компьютерных атак

Формирование из множества X множества X^* допустимых по стоимости вариантов построения системы защиты по критерию стоимости этой системы:

$$X^* = \left\{x_k^* | C(x_k^*) \le C_{\text{зад}}\right\}, x_k^* \in X, \tag{3.24}$$

где x_k^* – допустимый по стоимости вариант построения системы защиты, $C(x_k^*)$ – стоимость k-го варианта построения системы защиты, $C_{\text{зад}}$ – допустимая стоимость создания системы защиты.

Исходя из положения 1.4, стоимость каждого (j-го) альтернативного варианта построения системы защиты для каждого (i-го) уровня будет определяться как:

$$C\left(x_{ij}^0\right) = \sum_{h=1}^{H_i} C(s_{ih}). \tag{3.25}$$

Тогда стоимости всех альтернативных вариантов построения системы защиты для каждого уровня можно описать следующим образом:

$$\begin{gathered} C(X_{\text{уровн}}^{(1)}) \in \left\{C(x_{11}^0); C(x_{12}^0); \dots; C(x_{1J_1}^0)\right\} \\ C(X_{\text{уровн}}^{(2)}) \in \left\{C(x_{21}^0); C(x_{22}^0); \dots; C(x_{2J_2}^0)\right\} \\ \dots \\ C(X_{\text{уровн}}^{(N)}) \in \left\{C(x_{N1}^0); C(x_{N2}^0); \dots; C(x_{NJ_N}^0)\right\} \end{gathered} . \tag{3.26}$$

Для того чтобы сформировать один из вариантов системы защиты, допустимый по стоимости необходимо из множеств $X_{\text{уровн}}^{(1)}; X_{\text{уровн}}^{(2)}; \dots; X_{\text{уровн}}^{(N)}$ выбрать по одному элементу, таким образом, чтобы сумма стоимостей этих выбранных элементов не превышала допустимую стоимость $C_{\text{зад}}$.

Если число таких элементов обозначить T^*, то множество допустимых по стоимости вариантов построения системы защиты для АСУ в целом можно определить следующим образом:

$$X^* = \{x_1^*; x_2^*; \dots; x_{T^*}^*\}. \tag{3.27}$$

Для построения множества X^*, используя логическое выражение (3.17) можно определить булеву функцию следующего вида:

$$P_2 = \bigvee_{1 \le i \le T;\ 1 \le k_1 \le J_1;\ 1 \le k_2 \le J_2; \dots;\ 1 \le k_N \le J_N} \left(\left(x_{1k_1}^0 \wedge x_{2k_2}^0 \wedge \dots \wedge \wedge x_{Nk_N}^0 \right) \wedge \hat{C}_i \right), \tag{3.28}$$

где $\hat{C}_i$ – булева переменная, определяемая следующим образом:

$$\hat{C}_i = \begin{cases} 1, \text{если } \left(C\left(x_{1k_1}^0\right) + C\left(x_{2k_2}^0\right) + \dots + C\left(x_{Nk_N}^0\right) \right) \le C_{\text{зад}} \\ 0, \text{если } \left(C\left(x_{1k_1}^0\right) + C\left(x_{2k_2}^0\right) + \dots + C\left(x_{Nk_N}^0\right) \right) > C_{\text{зад}} \end{cases}, \tag{3.29}$$

при $i = \overline{1;T},\ k_1 = \overline{1;J_1},\ k_2 = \overline{1;J_2}, \dots,\ k_N = \overline{1;J_N}$.

Тогда число элементов множества X^* определяется как:

$$T^* = \sum_{i=1}^{T} \hat{C}_i. \tag{3.30}$$

Пример 3.2. Для условий примера 3.1 и при $C(x_{11}^0) = 2$, $C(x_{12}^0) = 1$, $C(x_{13}^0) = 2$, $C(x_{14}^0) = 3$, $C(x_{21}^0) = 4$, $C(x_{22}^0) = 3$, $C(x_{23}^0) = 5$, $C(x_{31}^0) = 3$, $C(x_{32}^0) = 5$, $C_{\text{зад}} = 9$ функция P_2 будет иметь следующий вид:

$$\begin{gathered} P_2 = \left((x_{11}^0 \wedge x_{21}^0 \wedge x_{31}^0) \wedge \hat{C}_1 \right) \vee \left((x_{11}^0 \wedge x_{21}^0 \wedge x_{32}^0) \wedge \hat{C}_2 \right) \vee \\ \vee \left((x_{11}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{C}_3 \right) \vee \left((x_{11}^0 \wedge x_{22}^0 \wedge x_{32}^0) \wedge \hat{C}_4 \right) \vee \left((x_{11}^0 \wedge x_{23}^0 \wedge x_{31}^0) \wedge \hat{C}_5 \right) \vee \\ \vee \left((x_{11}^0 \wedge x_{23}^0 \wedge x_{32}^0) \wedge \hat{C}_6 \right) \vee \left((x_{12}^0 \wedge x_{21}^0 \wedge x_{31}^0) \wedge \hat{C}_7 \right) \vee \left((x_{12}^0 \wedge x_{21}^0 \wedge x_{32}^0) \wedge \hat{C}_8 \right) \vee \\ \vee \left((x_{12}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{C}_9 \right) \vee \left((x_{12}^0 \wedge x_{22}^0 \wedge x_{32}^0) \wedge \hat{C}_{10} \right) \vee \left((x_{12}^0 \wedge x_{23}^0 \wedge x_{31}^0) \wedge \hat{C}_{11} \right) \vee \\ \vee \left((x_{12}^0 \wedge x_{23}^0 \wedge x_{32}^0) \wedge \hat{C}_{12} \right) \vee \left((x_{13}^0 \wedge x_{21}^0 \wedge x_{31}^0) \wedge \hat{C}_{13} \right) \vee \left((x_{13}^0 \wedge x_{21}^0 \wedge x_{32}^0) \wedge \hat{C}_{14} \right) \vee \\ \vee \left((x_{13}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{C}_{15} \right) \vee \left((x_{13}^0 \wedge x_{22}^0 \wedge x_{32}^0) \wedge \hat{C}_{16} \right) \vee \left((x_{13}^0 \wedge x_{23}^0 \wedge x_{31}^0) \wedge \hat{C}_{17} \right) \vee \\ \vee \left((x_{13}^0 \wedge x_{23}^0 \wedge x_{32}^0) \wedge \hat{C}_{18} \right) \vee \left((x_{14}^0 \wedge x_{21}^0 \wedge x_{31}^0) \wedge \hat{C}_{19} \right) \vee \left((x_{14}^0 \wedge x_{21}^0 \wedge x_{32}^0) \wedge \hat{C}_{20} \right) \vee \\ \vee \left((x_{14}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{C}_{21} \right) \vee \left((x_{14}^0 \wedge x_{22}^0 \wedge x_{32}^0) \wedge \hat{C}_{22} \right) \vee \left((x_{14}^0 \wedge x_{23}^0 \wedge x_{31}^0) \wedge \hat{C}_{23} \right) \vee \\ \vee \left((x_{14}^0 \wedge x_{23}^0 \wedge x_{32}^0) \wedge \hat{C}_{24} \right). \end{gathered} \tag{3.31}$$

Исходя из (3.29) $\hat{C}_1 = 1$, $\hat{C}_2 = 0$, $\hat{C}_3 = 1$, $\hat{C}_4 = 0$, $\hat{C}_5 = 0$, $\hat{C}_6 = 0$, $\hat{C}_7 = 1$, $\hat{C}_8 = 0$, $\hat{C}_9 = 1$, $\hat{C}_{10} = 1$, $\hat{C}_{11} = 1$, $\hat{C}_{12} = 0$, $\hat{C}_{13} = 1$, $\hat{C}_{14} = 0$,

$\hat{C}_{15} = 1$, $\hat{C}_{16} = 0$, $\hat{C}_{17} = 0$, $\hat{C}_{18} = 0$, $\hat{C}_{19} = 0$, $\hat{C}_{20} = 0$, $\hat{C}_{21} = 1$, $\hat{C}_{22} = 0$, $\hat{C}_{23} = 0$, $\hat{C}_{24} = 0$.

Тогда функция P_2 примет вид:

$$P_2 = (x_{11}^0 \wedge x_{21}^0 \wedge x_{31}^0) \vee (x_{11}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{12}^0 \wedge x_{21}^0 \wedge x_{31}^0) \vee \vee (x_{12}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{12}^0 \wedge x_{22}^0 \wedge x_{32}^0) \vee (x_{12}^0 \wedge x_{23}^0 \wedge x_{31}^0) \vee \vee (x_{13}^0 \wedge x_{21}^0 \wedge x_{31}^0) \vee (x_{13}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{14}^0 \wedge x_{22}^0 \wedge x_{31}^0). \quad (3.32)$$

Таким образом, множество допустимых по стоимости вариантов X^* будет выглядеть следующим образом:

$$X^* = \{x_1^* = \{x_{11}^0; x_{21}^0; x_{31}^0\}; x_2^* = \{x_{11}^0; x_{22}^0; x_{31}^0\}; x_3^* = \{x_{12}^0; x_{21}^0; x_{31}^0\}; x_4^* = \{x_{12}^0; x_{22}^0; x_{31}^0\}; x_5^* = \{x_{12}^0; x_{22}^0; x_{32}^0\}; x_6^* = \{x_{12}^0; x_{23}^0; x_{31}^0\}; x_7^* = \{x_{13}^0; x_{21}^0; x_{31}^0\}; x_8^* = \{x_{13}^0; x_{22}^0; x_{31}^0\}; x_9^* = \{x_{14}^0; x_{22}^0; x_{31}^0\}\}, \quad (3.33)$$

а число T^* элементов этого множества будет равно девяти**.**

3.2.3 Формирование предпочтительных вариантов построения системы защиты от компьютерных атак

Формирование множества X^{**} предпочтительных вариантов построения системы защиты по критерию эффективности системы защиты:

$$X^{**} = \{x_l^{**} | E(x_l^{**}) \geq E_{\text{треб}}\}, x_l^{**} \in X^*, \quad (3.34)$$

где x_l^{**} – предпочтительный вариант построения системы защиты, $E(x_l^{**})$ – эффективность *l*-го варианта построения системы защиты, $E_{\text{треб}}$ – требуемая эффективность системы защиты.

Если число таких элементов обозначить как T^{**}, то множество предпочтительных вариантов построения системы защиты для АСУ в целом можно определить следующим образом:

$$X^{**} = \{x_1^{**}; x_2^{**}; \ldots; x_{T^{**}}^{**}\}. \quad (3.35)$$

Положение 3.1. Эффективность системы защиты оценивается множеством *E* частных показателей:

$$E = \{e_1;\ e_2; \ldots; e_n\}. \tag{3.36}$$

Каждому элементу e_i множества E можно сопоставить один из элементов $e_{\text{треб}i}$ множества $E_{\text{треб}}$ требуемых значений i-го частного показателя, $i = \overline{1;n}$ (рисунок 3.4).

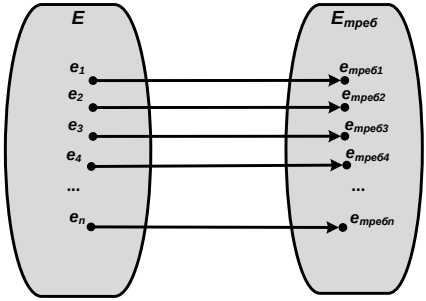


Рисунок 3.4 – Пример сопоставления элементов множества E элементам множества $E_{\text{треб}}$

Положение 3.2. Пусть Θ – множество тестовых процедур, позволяющих оценить эффективность системы защиты.

Тогда существует такой способ разработки тестовых процедур Φ_1, что каждому частному показателю из множества E соответствует тестовая процедура из множества Θ, т. е. такое соответствие из множества E в множество Θ (рисунок 3.5):

$$\begin{gathered}(\forall e \in E)(\forall \theta \in \Theta)(e\Phi_1\theta \Leftrightarrow \\ \Leftrightarrow (\text{частный показатель } e \text{ оценивается} \\ \text{тестовой процедурой } \theta)).\end{gathered} \tag{3.37}$$

При этом:

$$\left(\forall e_i, e_j \in E\right)\left(\left(i \neq j; e_i \neq e_j\right) \Rightarrow \left(\Phi_1(e_i) \neq \Phi_1(e_j)\right)\right), \tag{3.38}$$

т. е. различные частные показатели эффективности участвуют в разработке различных тестовых процедур, а также:

$$(\forall \theta_i \in \Theta)(\exists e_i \in E)(\Phi_1(e_i) = \theta_i), \tag{3.39}$$

т. е. любая тестовая процедура разрабатывается для оценки определенного частного показателя эффективности.

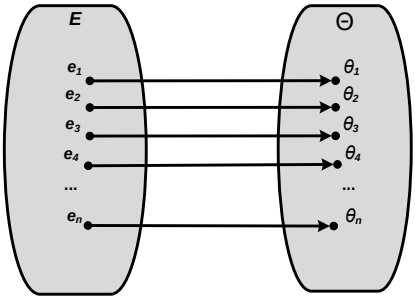


Рисунок 3.5 – Пример сопоставления элементов множества E элементам множества Θ

Введем булеву переменную ξ_i, т. е. переменную, принимающую значения из двухэлементного множества $\{0; 1\}$, которая будет показывать соответствие i-го частного показателя эффективности e_i, оцененного в результате проведения i-й тестовой процедуры θ_i, требуемому значению из множества $E_{\text{треб}}$.

Поскольку частные показатели эффективности могут быть выражены как в количественном виде, так и в качественном (в виде необходимости выполнения какого-либо требования), то для количественного выражения i-го частного показателя данная переменная будет определена следующим образом:

$$\xi_i = \begin{cases} 1, \text{если } e_i \geq e_{\text{треб}i} \\ 0, \text{в противном случае} \end{cases}, \tag{3.40}$$

а для качественного выражения i-го частного показателя:

$$\xi_i = \begin{cases} 1, \text{если требование } e_{\text{треб}i} \text{ выполнено} \\ 0, \text{в противном случае} \end{cases}. \tag{3.41}$$

Для автоматизированных систем управления технологическими процессами основной целью защиты от компьютерных атак является сохранение ее способности к штатному функционированию при реализации угроз безопасности. Под штатным режимом функционирования понимается соблюдение проектных пределов значений параметров выполнения целевых функций автоматизированной системы управления в условиях воздействия угроз безопасности [130]. Исходя из этого, в качестве показателя эффективности системы защиты от компьютерных атак возможно применение показателя

характеризующего способность сохранять проектные пределы значений параметров выполнения целевых функций автоматизированной системы управления в условиях воздействий компьютерных атак.

В качестве такого показателя предлагается использовать коэффициент сохранения эффективности выполнения возложенных на автоматизированную систему задач (функций).

Частными показателями эффективности системы защиты от компьютерных атак в этом случае будут являться коэффициенты сохранения эффективности выполнения отдельных задач (функций), возложенных на АСУ. Тогда множество частных показателей эффективности системы защиты можно представить в виде:

$$E = \left\{k_{\text{эфф}_1};\ k_{\text{эфф}_2}; \ldots; k_{\text{эфф}_n}\right\}, \tag{3.42}$$

где $k_{\text{эфф}_i}$ – коэффициент сохранения эффективности при выполнении АСУ i-й задачи (функции), $i = \overline{1;n}$, n – число задач (функций), возложенных на АСУ.

По аналогии с определением коэффициента сохранения эффективности, приведенном в [27] – коэффициент сохранения эффективности АСУ $k_{\text{эфф}_i}$ при выполнении i-й задачи (функции) в условиях воздействия на АСУ компьютерных атак можно представить в виде:

$$k_{\text{эфф}_i} = {e_{\text{асу}_i}}\Big/{e^0_{\text{асу}_i}}, \tag{3.43}$$

либо

$$k_{\text{эфф}_i} = {e^0_{\text{асу}_i}}\Big/{e_{\text{асу}_i}}, \tag{3.44}$$

где $e^0_{\text{асу}_i}$ – значение показателя, характеризующего эффективность выполнения i-й задачи (функции) без воздействия на АСУ компьютерных атак, $e_{\text{асу}_i}$ – значение показателя, характеризующего эффективность выполнения i-й задачи (функции) при воздействии на АСУ компьютерных атак.

При этом формулу (3.43) следует применять при ограничении значения показателя не ниже проектного, а формулу (3.45) – при ограничениях значения показателя не выше проектного.

Тестовой процедурой для оценки эффективности системы защиты при выполнении АСУ *i*-й задачи (функции) (в данном случае коэффициента снижения эффективности выполнения *i*-й задачи (функции)) будет являться процедура имитации возможных компьютерных атак в отношении защищаемой АСУ. Пример процедуры имитации компьютерной атаки вида «Локальный отказ в обслуживании» приведен в приложении Г.

Помимо сохранения возможности функционирования АСУ в штатном режиме в условиях воздействия на нее компьютерных атак, на систему защиты может быть возложена задача сохранения конфиденциальности информации, обрабатываемой или хранимой в АСУ.

В данном случае, применение каких-либо количественных показателей эффективности системы защиты (например, вероятности нарушения конфиденциальности, вероятности разглашения конфиденциальной информации и т. п.) затруднительно, поэтому эффективность системы защиты по сохранению конфиденциальности информации оценивается путем проверки выполнения системой защиты обязательных мер защиты, предусмотренных нормативными документами [116, 123].

Тогда *i*-й частный показатель эффективности системы защиты по обеспечению конфиденциальности информации будет определяться по итогам проверки наличия и корректности реализации *i*-й меры защиты в системе защиты (выражение (3.41)).

Тестовой процедурой в данном случае будет являться процедура проверки наличия и корректности реализации *i*-й меры защиты в системе защиты АСУ. Пример тестовой процедуры для проверки наличия и корректности меры защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» приведен в приложении Д.

Определение 3.1. Методикой оценки эффективности системы защиты будем называть функцию Ψ вида:

$$\Psi\left(S, \Theta_S, E_{S\text{зад}}\right) = \Xi, \qquad (3.45)$$

где S – оцениваемая система защиты, Θ_S – множество тестовых процедур, разработанных для оценки эффективности системы защиты S, $E_{S\text{зад}}$ – множество требуемых значений частных показателей эффективности системы защиты S, Ξ – двоичный набор длины $|\Theta_S|$, где $|\Theta_S|$ – число тестовых процедур в множестве Θ_S, т. е. набор значений переменной ξ, определенных по результатам проведения тестов Θ_S.

Тогда, исходя из положений 3.1 и 3.2 и определения 1.20 для формирования множества X^{**} предпочтительных вариантов построения системы защиты можно определить методику оценки эффективности, как функцию Ψ, в которой в качестве исходных данных – аргументов, будут использоваться допустимые по стоимости варианты построения системы защиты из сформированного ранее множества X^*; множество $\Theta_{X^{**}}$тестовых процедур для оценки эффективности варианта построения системы защиты и множество $E_{X^{**}\text{треб}}$ требуемых значений показателей эффективности системы защиты от компьютерных атак. Т. е. эта функция будет определяться следующим образом:

$$\Psi\left(x_i^*, \Theta_{X^{**}}, E_{X^{**}\text{треб}}\right) = \Xi_i, \tag{3.46}$$

где $i = \overline{1; T^*}$, T^* – число допустимых по стоимости вариантов построения системы защиты (множество X^*).

Результатом оценки эффективности в таком случае будет множество $\hat{\Xi}$ вида:

$$\hat{\Xi} = \{\Xi_1; \Xi_2; \dots; \Xi_{T^*}\}. \tag{3.47}$$

Множества $\Xi_1; \Xi_2; \dots; \Xi_i$ имеют вид:

$$\begin{gathered} \Xi_1 = \{\xi_{11}; \xi_{12}; \dots; \xi_{1n}\} \\ \Xi_2 = \{\xi_{21}; \xi_{22}; \dots; \xi_{2n}\} \\ \dots \\ \Xi_{T^*} = \{\xi_{T^*1}; \xi_{T^*2}; \dots; \xi_{T^*n}\} \end{gathered}, \tag{3.48}$$

где, как отмечалось ранее, ξ_{ij} – булева переменная, показывающая соответствие *j*-го частного показателя эффективности *i*-го варианта построения требованиям по эффективности системы защиты от компьютерных атак, $i = \overline{1; T^*}$, $j = \overline{1; n}$, n – число частных

показателей эффективности, необходимых для оценки эффективности системы защиты от компьютерных атак.

Тогда можно определить булевы переменные $\hat{\xi}_1; \hat{\xi}_2; \dots; \hat{\xi}_{T^*}$, которые показывают соответствие эффективности варианта построения системы защиты требуемому значению эффективности системы защиты в целом:

$$\hat{\xi}_i = \begin{cases} 1, \text{если } i\text{-й вариант построения системы защиты} \\ \quad \text{обеспечивает требуемую эффективность} \\ 0, \text{в противном случае} \end{cases}. \quad (3.49)$$

Значения данных переменных можно рассчитать следующим образом:

$$\hat{\xi}_i = \xi_{i1} \wedge \xi_{i2} \wedge \dots \wedge \xi_{in};\ i = \overline{1; T^*}. \quad (3.50)$$

Тогда для построения множества X^{**}, из множества X^* можно определить булеву функцию P_3 следующего вида:

$$P_3 = \bigvee_{1 \le i \le T^*} \left((x_i^*) \wedge \hat{\xi}_i \right), x_i^* \in X^*. \quad (3.51)$$

При этом число элементов множества X^{**} определяется как:

$$T^{**} = \sum_{i=1}^{T^*} \hat{\xi}_i. \quad (3.52)$$

Пример 3.3. Для множества X^*, сформированного в примере 3.2, при количестве частных показателей эффективности равном шести и исходя из следующих значений элементов множеств результатов оценки эффективности: $\Xi_1 = \{1; 1; 0; 1; 0; 1\}$; $\Xi_2 = \{1; 1; 1; 1; 1; 1\}$; $\Xi_3 = \{1; 0; 0; 1; 0; 0\}$; $\Xi_4 = \{1; 1; 1; 1; 1; 1\}$; $\Xi_5 = \{0; 1; 0; 1; 0; 0\}$; $\Xi_6 = \{1; 1; 0; 1; 1; 0\}$; $\Xi_7 = \{1; 1; 0; 1; 1; 1\}$; $\Xi_8 = \{1; 1; 1; 1; 1; 1\}$; $\Xi_9 = \{0; 1; 0; 0; 0; 0\}$ булева функция P_3 будет иметь вид:

$$\begin{aligned} P_3 = &\left((x_{11}^0 \wedge x_{21}^0 \wedge x_{31}^0) \wedge \hat{\xi}_1 \right) \vee \left((x_{11}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{\xi}_2 \right) \vee \\ \vee &\left((x_{12}^0 \wedge x_{21}^0 \wedge x_{31}^0) \wedge \hat{\xi}_3 \right) \vee \left((x_{12}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{\xi}_4 \right) \vee \\ \vee &\left((x_{12}^0 \wedge x_{22}^0 \wedge x_{32}^0) \wedge \hat{\xi}_5 \right) \vee \left((x_{12}^0 \wedge x_{23}^0 \wedge x_{31}^0) \wedge \hat{\xi}_6 \right) \vee \\ \vee &\left((x_{13}^0 \wedge x_{21}^0 \wedge x_{31}^0) \wedge \hat{\xi}_7 \right) \vee \left((x_{13}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{\xi}_8 \right) \vee \\ \vee &\left((x_{14}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \hat{\xi}_9 \right). \end{aligned} \quad (3.53)$$

Исходя из (3.50) $\hat{\xi}_1 = 0; \hat{\xi}_2 = 1; \hat{\xi}_3 = 0; \hat{\xi}_4 = 1; \hat{\xi}_5 = 0; \hat{\xi}_6 = 0; \hat{\xi}_7 = 0; \hat{\xi}_8 = 1; \hat{\xi}_9 = 0.$

Тогда P_3 примет следующий вид:

$$P_3 = (x_{11}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{12}^0 \wedge x_{22}^0 \wedge x_{31}^0) \vee (x_{13}^0 \wedge x_{22}^0 \wedge x_{31}^0). \quad (3.54)$$

Таким образом, множество предпочтительных вариантов X^{**} будет выглядеть следующим образом:

$$X^{**} = \{x_1^{**} = \{x_{11}^0; x_{22}^0; x_{31}^0\}; x_2^{**} = \{x_{12}^0; x_{22}^0; x_{31}^0\}; x_3^{**} = \{x_{13}^0; x_{22}^0; x_{31}^0\}\}, \quad (3.55)$$

а число T^{**} элементов этого множества будет равно трем.

3.2.4 Выбор оптимального варианта построения системы защиты от компьютерных атак

Выбор из множества X^{**} оптимального варианта $x_{\text{опт}}$ построения системы защиты по критерию минимального влияния системы защиты на производительность защищаемой системы:

$$x_{\text{опт}} = argmin\,(K(x_m^{**})), x_m^{**} \in X^{**}, \quad (3.56)$$

где $x_{\text{опт}}$ – оптимальный вариант построения системы защиты, $K(x_m^{**})$ – коэффициент влияния m-го варианта x_m^{**} построения системы защиты на производительность защищаемой автоматизированной системы управления.

Положение 3.3. Пусть автоматизированная система управления предназначена для выполнения определенного числа функций (задач). Тогда эти функции (задачи), образуют множество выполняемых функций (задач) Ω, и каждому элементу ω_i этого множества можно сопоставить весовой коэффициент важности σ_i, характеризующий важность выполнения i-й функции (задачи) в рамках целевого предназначения автоматизированной системы такой, что:

$$\sigma_1 + \sigma_2 + \cdots + \sigma_Y = 1. \quad (3.57)$$

В общем случае это можно представить в виде отображения множества Ω на множество Σ (рисунок 3.6).

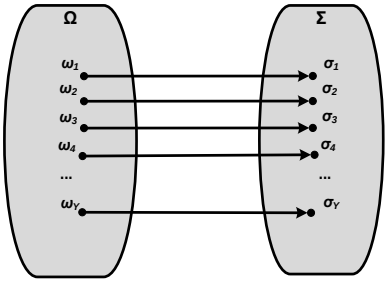


Рисунок 3.6 – Пример сопоставления элементов множества Ω элементам множества Σ

Определение 3.2. Методикой оценки снижения производительности автоматизированной системы управления, защищенной системой защиты S, при решении ею задачи ω будем называть функцию вида:

$$\Upsilon(S, \omega) = \Delta\pi. \tag{3.58}$$

Результатом оценки снижения производительности автоматизированной системы для всего множества выполняемых ею функций (задач) Ω будет являться множество ΔП вида:

$$\Delta\Pi = \{\Delta\pi_1; \Delta\pi_2; \dots; \Delta\pi_Y\}, \tag{3.59}$$

где Y – число функций (задач), выполняемых автоматизированной системой управления.

Пример методики оценки снижения производительности автоматизированной системы для антивирусных средств защиты приведен в [48, 106].

Положение 3.4. Множество ΔП является отображением множества Ω. Тогда, исходя из положения 3.4, множество ΔП также является отображением множества Σ (рисунок 3.7).

Тогда, общее снижение $\Delta\hat{\pi}_S$ производительности автоматизированной системы, при введении в ее состав системы защиты S можно определить как:

$$\Delta\hat{\pi}_s = \sum_{i=1}^{Y} \Delta\pi_{S_i}\sigma_i, \tag{3.60}$$

где $\Delta\pi_{S_i}$ – снижение производительности автоматизированной системы, оснащенной системой защиты S, при решении ею i-й задачи.

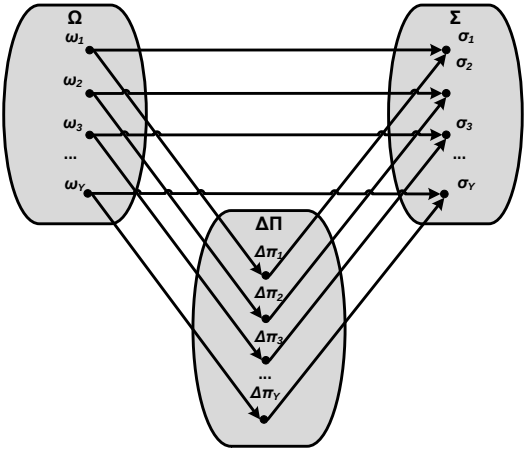


Рисунок 3.7 - Пример сопоставления элементов множества ΔП элементам множества Σ

Тогда, исходя из положения 3.4 и определения 1.21 для выбора оптимального варианта построения системы защиты $x_{\text{опт}}$ из множества X^{**} предпочтительных вариантов построения системы защиты можно определить методику оценки снижения производительности, в которой в качестве исходных данных будут использоваться предпочтительные варианты построения системы защиты из сформированного ранее множества X^{**}, следующим образом:

$$\Upsilon\left(x_i^{**}, \omega_j\right) = \Delta\pi_{ij}, \tag{3.61}$$

где $i = \overline{1; T^{**}}$, T^{**} – число предпочтительных вариантов построения системы защиты (т. е. число элементов множества X^{**}), $j = \overline{1; Y}$, Y – число задач возложенных на автоматизированную систему.

Результатом оценки эффективности в таком случае будет совокупность множеств $\Delta\Pi_i$ вида:

$$\begin{gathered}\Delta\Pi_1 = \{\Delta\pi_{11}; \Delta\pi_{12}; \dots; \Delta\pi_{1Y}\} \\ \Delta\Pi_2 = \{\Delta\pi_{21}; \Delta\pi_{22}; \dots; \Delta\pi_{2Y}\} \\ \dots \\ \Delta\Pi_{T^{**}} = \{\Delta\pi_{T^{**}1}; \Delta\pi_{T^{**}2}; \dots; \Delta\pi_{T^{**}Y}\}\end{gathered}. \tag{3.62}$$

Исходя из (3.60) можно определить показатели общего снижения производительности автоматизированной системы при введении в ее состав системы защиты, построенной на основе i-го варианта x_i^{**}:

$$\Delta\hat{\pi}_i = \sum_{j=1}^{Y} \Delta\pi_{ij}\sigma_j, i = \overline{1; T^{**}}. \quad (3.63)$$

Полученные значения $\Delta\hat{\pi}_i$ образуют множество $\Delta\hat{\Pi}$ вида:

$$\Delta\hat{\Pi} = \{\Delta\hat{\pi}_1; \Delta\hat{\pi}_2; \dots; \Delta\hat{\pi}_{T^{**}}\}. \quad (3.64)$$

Введем булеву переменную τ_i, которую определим следующим образом:

$$\tau_i = \begin{cases} 1, \text{если } \Delta\hat{\pi}_i = min(\Delta\hat{\Pi}) \\ 0, \text{в противном случае} \end{cases}. \quad (3.65)$$

Тогда для выбора оптимального варианта построения системы защиты из множества X^{**} можно определить булеву функцию P_4 следующего вида:

$$P_4 = \bigvee_{1 \le i \le T^{**}} \left((x_i^{**}) \wedge \tau_i\right), x_i^{**} \in X^{**}. \quad (3.66)$$

Пример 3.4. Для множества X^{**}, сформированного в примере 3.3, и числе задач равном трем, при $\Sigma = \{0{,}3; 0{,}5; 0{,}2\}$, $\Delta\Pi_1 = \{0{,}7; 0{,}9; 0{,}3\}$, $\Delta\Pi_2 = \{0{,}4; 0{,}2; 0{,}7\}$, $\Delta\Pi_3 = \{0{,}8; 0{,}1; 0{,}4\}$ булева функция P_4 будет иметь вид:

$$P_4 = \left((x_{11}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \tau_1\right) \vee \left((x_{12}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \tau_2\right) \vee \vee ((x_{13}^0 \wedge x_{22}^0 \wedge x_{31}^0) \wedge \tau_3). \quad (3.67)$$

Исходя из выражения (3.60), множество $\Delta\hat{\Pi} = \{0{,}72; 0{,}36; 0{,}37\}$. Тогда из (3.65) следует $\tau_1 = 0, \tau_2 = 1, \tau_3 = 0$, и функция P_4 примет вид:

$$P_4 = (x_{12}^0 \wedge x_{22}^0 \wedge x_{31}^0). \quad (3.68)$$

Таким образом оптимальным вариантом построения системы защиты будет являться вариант:

$$x_{\text{опт}} = \{x_{12}^0; x_{22}^0; x_{31}^0\}. \quad (3.69)$$

Как видно из вышеизложенного построение системы защиты от компьютерных атак для автоматизированных систем управления представляет собой процесс поэтапного выбора оптимальной структуры системы защиты и включает в себя:

– этап формирования множества всех возможных вариантов построения системы защиты;

– этап формирования множества альтернативных вариантов построения системы защиты;

– этап формирования множества предпочтительных вариантов построения системы защиты;

– этап выбора из сформированного множества предпочтительных вариантов, оптимального варианта построения системы защиты.

Предложенный подход позволит на основе ранее сформированных функциональных требований к системе защиты от компьютерных атак осуществить синтез оптимальной структуры системы защиты от компьютерных атак. Полученный в результате вариант построения системы защиты будет удовлетворять функциональным требованиям, требованиям по эффективности защиты, а также будет оказывать минимальное влияние на производительность (а следовательно, и на качество функционирования) защищаемой АСУ.

Заключение

В данной работе получили дальнейшее развитие научно-теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления.

Проанализировано современное состояние вопросов защиты информационно-вычислительных (автоматизированных) систем различного назначения от компьютерных атак, а также изложены методологические основы защиты информации в информационно-вычислительных (автоматизированных) системах и обеспечения их безопасного функционирования в условиях различных информационно-технических воздействий (в том числе и в условиях компьютерных атак).

Уточнен и определен понятийный аппарат, касающийся вопросов защиты автоматизированных систем управления от компьютерных атак.

Показано, что выбор оптимального варианта построения системы защиты от компьютерных атак является сложной многокритериальной задачей принятия решения.

Разработаны и предложены теоретико-методологические подходы к решению задачи формирования перечня актуальных для защищаемой автоматизированной системы управления компьютерных атак, задачи формирования функциональных требований к системе защиты, а также задачи выбора оптимального (с точки зрения потребляемых ресурсов защищаемой системы) варианта построения системы защиты.

Представленные в монографии теоретико-методологические подходы могут быть использованы для обоснования функциональных требований к системам защиты от компьютерных атак, а также выбора оптимального варианта построения систем защиты от компьютерных атак для автоматизированных систем управления.

Литература

1. Common Vulnerability Scoring System [Электронный ресурс]. – URL: http://www.first.org/cvss (дата обращения 25.09.2017).
2. Алгулиев Р. М. Методы синтеза адаптивных систем обеспечения информационной безопасности корпоративных сетей / Р. М. Алгулиев. – М.:УРСС, 2001. – 248 с.
3. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность / А. С. Алпеев // Вопросы кибербезопасности. 2014. №5 (8). С. 39 – 42.
4. Астахов А. Анализ защищенности корпоративных систем [Электронный ресурс] // Открытые системы. СУБД. 2002. №7,8. URL: http://www.osp.ru/os/2002/07-08/181720 (дата обращения 25.09.2017).
5. Банк данных угроз информационной безопасности. Список угроз [Электронный ресурс] // ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: http://www.bdu.fstec.ru/threat (дата обращения 25.08.2017).
6. Банк данных угроз информационной безопасности. Список уязвимостей [Электронный ресурс] // ФАУ «ГНИИИ ПТЗИ ФСТЭК России». – URL: http://www.bdu.fstec.ru/vul (дата обращения 25.08.2017).
7. Баранова Е. К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. 2015. №1 (9). С. 73 – 79.
8. Батутов А. Экономический взгляд на проблемы информационной безопасности [Электронный ресурс] // Открытые системы. 2002. №7, 8. URL: https://www.osp.ru/os/2002/02/181118 (дата обращения 25.08.2017)
9. Бедрань А. Эшелонированная антивирусная защита / А. Бедрань // IT-Expert. 2011. №7 – 8 (194). С. 56 – 59.
10. Безопасность АСУ ТП в цифрах [Электронный ресурс] // Positive Technologies. 2016. URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Vulnerability-2016-rus.pdf (дата обращения 25.09.2017).
11. Безопасность АСУ ТП: итоги 2016 года [Электронный ресурс] // Positive Technologies. 2017.

URL: https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-rus.pdf (дата обращения 25.09.2017).

12. Белов В. Терминологическая база теории безопасности / В. Белов, А. Голяков // Стандарты и качество. 2004. №9. С. 48 – 51.

13. Белоножкин В. И., Остапенко Г. А. Информационные аспекты противодействия терроризму. – М.: Горячая линия-Телеком, 2009. – 112 с.

14. Бирюков А. Стеганография: Реализация и предотвращение / А. Бирюков // Системный администратор. 2015. №4 (149). С. 24 – 27.

15. Бойко А. А., Е. Ю. Обущенко, А. В. Щеглов. Особенности синтеза полного множества тестовых способов удаленного информационно-технического воздействия на пространственно распределенные системы информационно-технических средств // Вестник ВГУ, серия: Системный анализ и информационные технологии. 2017. № 2. С. 33 – 45.

16. Бородакий Ю. В., Добродеев А. Ю., Бутусов И. В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) // Вопросы кибербезопасности. 2013. № 1 (1). С. 2 – 9.

17. Бородакий Ю. В., Добродеев А. Ю., Коротков И. К., Вакуленко А. А. Проблемные вопросы создания адаптивных систем защиты информации. Материалы 7 Международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТРТУ, 2005, с. 33 – 36.

18. Будников С. А., Паршин Н. В. Информационная безопасность автоматизированных систем. – Воронеж: ГУП ВО «Воронежская областная типография – издательство им. Е. А. Болховитинова», 2011. – 354 с.

19. Буренин А. Н., Легков К. Е. Современные инфокоммуникационные системы и сети специального назначения. Основы построения и управления. – М.: ООО «Издательский дом Медиа паблишер», 2015. – 348 с.

20. Быков А. А. О взаимосвязи риска с родственными понятиями и терминологии риск-менеджмента / А. А. Быков, Б. Н. Порфирьев // Проблемы анализа риска. 2013. Том 10, № 4. С. 4 – 10.

21. Галатенко В. А. Стандарты информационной безопасности: курс лекций: учебное пособие / под редакцией академика РАН В. Б. Бетелина. – М.: ИНТУИТ.РУ, 2006. – 264 с.

22. Гамаюнов Д. Ю. Обнаружение компьютерных атак на основе анализа поведения сетевых объектов: дис. … канд. физ. мат. наук: 05.13.11 / Д. Ю. Гамаюнов. – М.: Московский государственный университет им. М. В. Ломоносова, 2007. – 89 с.

23. Гаценко О. Ю. Защита информации. Основы организационного управления. – СПб.: Изд. дом «Сентябрь», 2001. – 208 с.

24. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, кн. 1 и 2, 1994.

25. Герасименко В. А., Малюк А. А. Основы защиты информации. – М.: МИФИ, 1997. – 537 с.

26. ГОСТ 24.701 – 86. Единая система стандартов автоматизированных систем управления. Надежность автоматизированных систем управления. Основные положения. – М.: Издательство стандартов, 1986. – 64 с.

27. ГОСТ 27.002 – 2015. Надежность в технике. Термины и определения. М.: Стандартинформ, 2015. – 23 с.

28. ГОСТ 27.310 – 95. Надежность в технике. Анализ видов, последствий и критичности отказов. Основные положения. – М.: Издательство стандартов, 1995. – 24 с.

29. ГОСТ 34.003 – 90. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения. – М.: Издательство стандартов, 1992. – 38 с.

30. ГОСТ 34.12 – 2015. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2015. – 25 с.

31. ГОСТ 34.13 – 2015. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2015. – 42 с.

32. ГОСТ Р 50922 – 2006. Защита информации. Термины и определения. – М.: Стандартинформ, 2006. – 18 с.

33. ГОСТ Р ИСО/МЭК 15408 – 1 – 2012. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Часть 1. Введение и общая модель. – М.: Стандартинформ, 2014. – 88 с.

34. ГОСТ Р ИСО/МЭК 15408 – 2 – 2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные компоненты безопасности. – М.: Стандартинформ, 2014. – 161 с.

35. ГОСТ Р ИСО/МЭК 15408 – 3 – 2013. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. – М.: Стандартинформ, 2014. – 274 с.

36. Гречишников Е. В., Добрышин М. М. Оценка эффективности деструктивных программных воздействий на сети связи / Е. В. Гречишников, М. М. Добрышин // Системы управления, связи и безопасности. 2016. №2. С. 135 – 146.

37. Гриняев С. Н. Интеллектуальное противодействие информационному оружию. – М.: СИНТЕГ, 1999. – 232 с.

38. Гриняев С. Н. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны. – М.: Харвест, 2004. – 426 с.

39. Гриняев С. Н. Системы обнаружения вторжений и реагирования на компьютерные инциденты на основе мобильных программ-агентов. – М.: АНО ЦСОиП, 2005. – 46 с.

40. Гришина Н. В. Модель потенциального нарушителя объекта информатизации / Н. В. Гришина // Известия ЮФУ. Технические науки. 2003. №4, Том 33. С. 356 – 358.

41. Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. – М.: Изд-во агентства «Яхтсмен», 1996. – 73 с.

42. Девянин П. Н. Модели безопасности компьютерных систем: Учебное пособие для студ. высш. учеб. заведений / П. Н. Девянин. – М.: Издательский центр «Академия», 2005. – 144 с.

43. Дементьев В. Е., Коцыняк М. А., Стародубцев Ю. И. Комплексная защита информации в локальных вычислительных сетях / Под общ. ред. Ю. М. Ровчака. – СПб.: Военная академия связи им. С. М. Буденного, 2010. 435 с.

44. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. – Киев: ООО «ТИД «ДС», 2002. – 688 с.

45. Дроботун Е. Б. База данных угроз информационной безопасности и уязвимостей компонентов информационно-вычислительных систем: Свидетельство о государственной регистрации базы данных / Е. Б. Дроботун, А. С. Марковский, В. П. Бердышев. – №2016620378, заявл. 02.02.2016, зарег. 24.03.2016.

46. Дроботун Е. Б., Бердышев В. П. Защита автоматизированных систем управления военного назначения от разрушающих программных воздействий / Е. Б. Дроботун, В. П. Бердышев // Военная мысль. 2016. №10. С. 15 – 19.

47. Дроботун Е. Б., Бердышев В. П. Морозов А. В. Оценка эффективности реализации угроз безопасности информации в автоматизированных системах военного назначения с учетом потенциала противника / Е. Б. Дроботун, В. П. Бердышев, А. В. Морозов // Вестник Военной академии воздушно-космической обороны. 2016. №1. С. 80 – 95.

48. Дроботун Е. Б., Козлов Д. В. Оценка степени влияния антивирусных программных средств на качество функционирования информационнно-вычислительных систем / Е. Б. Дроботун, Д. В. Козлов // Программные продукты и системы. 2016. №4 (том 29). С. 129 – 134.

49. Дроботун Е. Б. Об определении компьютерного вируса и вредоносной программы // Сборник материалов IX Международной научно-технической конференции «Новые информационные технологии и системы 2010». – Пенза, 2010. – С. 104 – 107.

50. Дроботун Е. Б. Программа оценки потенциала нарушителя безопасности информации: Свидетельство о государственной регистрации программы для ЭВМ / Е. Б. Дроботун, О. В. Цветков, А. С. Марковский. – №2016615110, заявл. 24.03.2016, зарег. 16.05.2016.

51. Дроботун Е. Б. Риск-ориентированный подход к формированию функциональных требований к системам защиты от компьютерных атак для автоматизированных систем управления: монография. – Тверь: Издатель А. Н. Кондратьев, 2017. – 195 с.: ил.

52. Дроботун Е. Б. Синтез систем защиты автоматизированных систем управления от разрушающих

программных воздействий / Е. Б. Дроботун // Программные продукты и системы. 2016. №3 (115). С. 51 – 59.

53. Дроботун Е. Б., Угловский Е. П., Замалтдинов И. Ш. Метод формирования множеств альтернативных вариантов построения подсистем, входящих в состав системы защиты от компьютерных атак / Е. Б. Дроботун, Е. П. Угловский, И. Ш. Замалтдинов // Программные продукты и системы. 2017. №2 (том 30). С. 314 – 319.

54. Дроботун Е. Б., Цветков О. В. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действий нарушителя / Е. Б. Дроботун, О. В. Цветков // Программные продукты и системы. 2016. №3 (115). С. 42 – 50.

55. Емелин В. И. Методы и модели оценки и обеспечения информационной безопасности автоматизированных систем управления критическими системами: дис. … докт. техн. наук: 05.13.19 / В. И. Емелин. – СПб.: СПИИРАН, 2012. – 239 с.

56. Жуков В. Г. Модель нарушителя прав доступа в автоматизированной системе / В. Г. Жуков, М. Н. Жукова, А. П. Стефаров // Программные продукты и системы. 2012. №2 (98). С. 75 – 78.

57. Жуматий В. П., Будников С. А., Паршин Н. В. Угрозы программно-математического воздействия. – Воронеж: ГУП ВО «Воронежская областная типография – издательство им. Е. А. Болховитинова», 2010. – 231 с.

58. Зайцев О. В. Rootkits, Spyware/Adware, Keyloggers & Backdoors: обнаружение и защита. – СПб.: БХВ-Петербург, 2006. 304 с.: ил.

59. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Котенко И. В., Котухов М. М., Марков А. С., Карпов Е. А., Парр Г. А., Рунеев А. Ю.: под ред. Котенко И. В. – СПб.: Военная академия связи им. С. М. Буденного, 2000. – 190 с.

60. Зегжда Д. П., Ивашко А. М. Основы безопасности информационных систем. – М.: Горячая линия-Телеком, 2000. – 452 с, ил.

61. Зегжда Д. П. Принципы и методы создания защищенных систем обработки информации: дис. … докт. техн. наук: 05.13.19 /

Д. П. Зегжда. – СПб.: Санкт-Петербургский государственный политехнический университет, 2002. – 380 с.

62. Зикратов И. А., Одегов С. В., Смирных А. В. Оценка рисков информационной безопасности в облачных сервисах на основе линейного программирования / И. А. Зикратов, С. В. Одегов, А. В. Смирных // Научно-технический вестник информационных технологий, механики и оптики. 2013. №1 (89). С. 141 – 144.

63. Зима В. М., Молдавян А. А., Молдавян Н. А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2000. – 320 с.: ил.

64. Иванов К. В., Тутубалин П. И. Марковские модели защиты автоматизированных систем специального назначения: монография. – Казань: ГБУ «Республиканский центр мониторинга качества образования», 2012. – 216 с.: ил.

65. Иванов М. А. Разработка и исследование стохастических методов и средств защиты программных систем ответственного назначения: дис. … докт. техн. наук: 05.13.11, 05.13.19 / М. А. Иванов. – М.: Московский инженерно-физический институт, 2005. – 267 с.

66. Информационные риски флуд-атакуемых компьютерных систем: Монография/ В. В. Бутузов, М. В. Бурса, А. Г. Остапенко, А. О. Калашников, Г. А. Остапенко; под ред. чл.-корр. РАН Д. А. Новикова. – Воронеж: Издательство «Научная книга», 2015. – 160 с.

67. Казарин О. В. Безопасность программного обеспечения компьютерных систем. Монография. – М.: МГУЛ, 2003. – 212 с.

68. Карвальо М., Форд Р. Защита сетей путем создания движущихся целей // Открытые системы СУБД. 2014. №4. С. 36 – 38.

69. Карпычев В. Ю. Экономический анализ нормативно-технического обеспечения информационной безопасности / В. Ю. Карпычев // Экономический анализ: теория и практика. 2011. №35 (242). С. 2 – 18.

70. Кибербезопасность промышленных систем: ландшафт угроз [Электронный ресурс] // АО «Лаборатория Касперского». 2016. URL: https://securelist.ru/industrial-cybersecurity-threat-landscape/28866 (дата обращения 25.09.2017).

71. Киберустойчивость информационно-телекоммуникационной сети: монография / М. А. Коцыняк, И. А. Кулешов, А. М. Кудрявцев, О. С. Лаута. – СПб.: Бостон-спектр, 2015. – 150 с.

72. Климов С. М. Методы и модели противодействия компьютерным атакам. – Люберцы.: КАТАЛИТ, 2008. – 316 с.

73. Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Методические основы: Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. – 108 с.

74. Климов С. М., Сычев М. П., Астрахов А. В. Противодействие компьютерным атакам. Технологические основы: Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. – 70 с.

75. Климов С. М., Сычев М. П., Астрахов А. В. Экспериментальная оценка противодействия компьютерным атакам на стендовом полигоне: Электронное учебное издание. – М.: МГТУ имени Н.Э. Баумана, 2013. – 108 с.

76. Козирацкий Ю. Л., Ерофеев А. Н., Соколовский С. П. Модель конфликтного взаимодействия «нарушитель-подсистема защиты информации автоматизированной системы управления» // Вестник Военного авиационного инженерного университета. 2012. № 1 (15). С. 210 – 217.

77. Козирацкий Ю. Л., Ухин А. Л. Вероятностная модель конфликта радиоэлектронных систем управления и телекоммуникации в условиях деструктивных воздействий // Системы управления и информационные технологии. 2014. №3.2(57). С. 281 – 286.

78. Компьютерная безопасность на ядерных установках. Справочное издание. – Вена: Международное агентство по атомной энергии, 2013. – 80 с.

79. Корченко А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – Киев.: «МК-Пресс», 2006. – 390 с.

80. Котенко И. В., Саенко И. Б. Построение системы интеллектуальных сервисов для защиты информации в условиях кибернетического противоборства // Труды СПИИРАН. 2012. №3 (22). С. 84 – 100.

81. Котенко И. В., Чечулин А. А., Федорченко А. В. Исследование открытых баз уязвимостей и оценка возможности их применения в системах анализа защищенности компьютерных сетей / И. В. Котенко, А. А. Чечулин, А. В. Федорченко // Информационно-управляющие системы. 2014. №5. С. 72 – 79.

82. Липаев В. В. Надежность и функциональная безопасность комплексов программ реального времени: монография / В. В. Липаев. – М.; Берлин: Директ-Медиа, 2015. – 281 с.: ил.

83. Ломако А. Г., Еремеев М. А., Новиков В. А. Метод выявления дефектов и недокументированных возможностей программ / А. Г. Ломако, М. А. Еремеев, В. А. Новиков // Информационное противодействие угрозам терроризма. 2010. №14. С. 46 – 49.

84. Лукинова О. В. Компьютерные модели и алгоритмы управления безопасностью информационных систем: дис. … докт. техн. наук: 05.13.11, 05.13.19 / О. В. Лукинова. – М.: Институт проблем управления им. В. А. Трапезникова РАН, 2013. – 296 с.

85. Макаренко С. И. Информационное оружие в технической сфере: терминология, классификация, примеры [Электронный ресурс] // Системы управления, связи и безопасности. 2016. №3. С. 292 – 376. URL: http://sccs.intelgr.com/archive/2016-03/11-Makarenko.pdf (дата обращения 25.09.2017)

86. Макаренко С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. – СПб.: Наукоемкие технологии, 2017. – 546 с.

87. Малюк А. А. Введение в защиту информации в автоматизированных системах / А. А. Малюк, С. В. Пазизин, Н. С. Пригожин. – М.: Горячая линия-Телеком, 2001. – 148 с.: ил.

88. Малюк А. А. Информационная безопасность: концептуальные и методологические основы защиты информации. Учеб. пособие для вузов. – М.: Горячая линия-Телеком, 2004. – 208 с.: ил.

89. Мамиконов А. Г. Достоверность, защита и резервирование информации в АСУ / А. Г. Мамиконов, В. В. Кульба, А. Б. Шелков. – М.: Энергоатомиздат, 1986. – 304 с.

90. Марков А. С., Цирлов В. Л., Барабанов А. В. Методы оценки несоответствия средств защиты информации / А. С. Марков, В. Л. Цирлов, А. В. Барабанов; под ред. А. С. Маркова. – М.: Радио и связь, 2012. – 192 с.

91. Медведовский И. Д., Семьянов П. В., Леонов В. В. Атака через Интернет. Под научной редакцией проф. Зегжды П. Д. – СПб.: НПО «Мир и семья – 95 », 1997. – 296 с.

92. Методический документ. Меры защиты информации в государственных информационных системах: утв. ФСТЭК России 11 февраля 2014 г. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/675 (дата обращения 25.09.2017).

93. Новиков В. А., Компаниец Р. И., Ломако А. Г. «Спецпроверка» программ / В. А. Новиков, Р. И. Компаниец, А. Г. Ломако // Защита информации. Инсайд. 2006. №3 (9). С. 18 – 27.

94. Новиков С. Н. Методология защиты информации на основе технологий сетевого уровня мультисервисных сетей связи: дис. … докт. техн. наук: 05.13.19 / С. Н. Новиков. – Новосибирск.: СибГути, 2016. – 235 с.

95. Нурдинов Р. А. Определение вероятности нарушения критических свойств информационного актива на основе CVSS метрик уязвимостей [Электронный ресурс] / Современные проблемы науки и образования. 2014. №3. URL: https://elibrary.ru/download/elibrary_22527869_57606179.pdf (дата обращения 25.09.2017).

96. Оптимальный синтез и анализ эффективности комплексов средств защиты информации: Монография / В. Г. Кулаков, В. Г. Кобящев и др.; науч. редакторы : Я. Е. Львович, А. Г. Остапенко. – Воронеж: ВГТУ, 2006. – 137с.

97. Основы проектирования и эксплуатации автоматизированных систем управления военного назначения: учеб. пособие / под ред. доктора технических наук, профессора В. Л. Лясковского. – М.: Издательство МГТУ им. Н. Э. Баумана, 2016. – 188, [2] с.: ил.

98. Остапенко Г. А., Ермилов Е. В., Калашников А. О. Построение функций ущерба и риска для компьютерных атак, приводящих к нарушению доступности к информации / Г. А. Остапенко, Е. В. Ермилов, А. О. Калашников // Информация и безопасность. 2013. Том. 16. №2. С. 207 – 210.

99. Остапенко Г. А. Информационные риски в социальных сетях: Монография / Г. А. Остапенко, Л. В. Паринова, В. И. Белоножкин, И Л. Батаронов, К. В. Симонов; под ред. чл.-

корр. РАН Д. А. Новикова. – Воронеж: Издательство «Научная книга». 2013. – 160 с.

100. Пат. 2263950 Российская Федерация, МПК G06F 12/14 (2000.01). Устройство защиты от несанкционированного доступа к информации, хранимой в персональной ЭВМ / Бородакий Ю. В., Добродеев А. В., Свиридюк Ю. П., Терешкин Н. Л. – 2003134384, заявл. 28.11.2003, опубл. 10.11.2005, Бюл. №14. – 14 с.

101. Пат. 2316810 Российская Федерация, МПК G06F 11/30 (2006.01). Устройство активной защиты и обеспечения технической готовности элементов распределенной локальной вычислительной сети в условиях внешних деструктивных воздействий / Гречишников Е. В., Иванов В. А., Двилянский А. А., Белов А. С. – 2006106880, заявл. 06.03.2006, опубл. 10.02.2008, Бюл. №4. – 17 с.

102. Пат. 2443017 Российская Федерация, МПК G06F 21/22 (2006.01), G06F 12/14 (2006.01). Система защиты информации от несанкционированного доступа к информации, содержащей сведения, составляющие государственную тайну / Бородакий Ю. В., Бельтов А. Г., Добродеев А. В., Коротков С. В., Нащекин П. А., Непомнящих А. В., Соколов И. А. – 2010131860, заявл. 30.07.2010, опубл. 20.02.2012, Бюл. №5. – 16 с.

103. Пат. 2451416 Российская Федерация, МПК H04L 29/14 (2006.01). Способ (варианты) защиты системы связи от внешних деструктивных воздействий / Гречишников Е. В., Стародубцев Ю. И., Белов А. С., Гусев А. П. – 2011115902, заявл. 21.04.2011, опубл. 20.05.2012, Бюл. №14. – 20 с.

104. Пат. 2623721 Российская Федерация, МПК G06F 21/00 (2013.01). Способ проектирования и построения системы защиты автоматизированных систем управления критически важными объектами от разрушающих программных воздействий / Дроботун Е. Б. – 2016100332, заявл. 11.01.2016, опубл. 28.06.2017, Бюл. 19. – 2 с.

105. Пат. 2627386 Российская Федерация, МПК G06F 21/57 (2013.01). Стенд для испытаний автоматизированных систем в условиях воздействия вредоносных программ / Дроботун Е. Б. – 2016123658, заявл. 14.06.2016, опубл. 10.08.2017, Бюл. 22. – 2 с.

106. Пат. 2628899 Российская Федерация, МПК G06F 21/00 (2013.01). Способ оценки степени влияния антивирусных программных средств на качество функционирования

информационно-вычислительных систем / Дроботун Е. Б. – 2016119303, заявл. 18.05.2016, опубл. 22.08.2017, Бюл. 24. – 2 с.

107. Пашковская Е. С., Пашковский М. Е., Барабанов В. Ф. Построение «периметровой» стратегии защиты информационных систем персональных данных на основе настроек межсетевого экрана Netfilter / Е. С. Пашковская, М. Е. Пашковский, В. Ф. Барабанов // Вестник Воронежского государственного технического университета. 2012. Том 8, №4. С. 39 – 43.

108. Петренко С. А. Методы информационно-технического воздействия на киберсистемы и возможные способы противодействия // Труды Института системного анализа Российской академии наук. 2009. Том 41. С. 104 – 146.

109. Петренко С. А., Ступин Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / С. А. Петренко, Д. Д. Ступин // под общей редакцией С. Ф. Боева. Университет Иннополис. – Иннополис: «Издательский Дом «Афина», 2017. – 440 с.

110. Пугин В. В. Обзор методик анализа рисков информационной безопасности информационной системы предприятия / В. В. Пугин, О. Ю. Губарева // T-Comm. 2012. №6. – С. 54 – 57.

111. Разработка систем информационно-компьютерной безопасности / В. М. Зима, М. М. Котухов, А. Г. Ломако, А. С. Марков, А. А. Молдовян. – СПб.: Военно-космическая академия им. А. Ф. Можайского, 2003. – 327 с.

112. Разрушающие программные воздействия: Учебно-методическое пособие / А. Б. Вавренюк, Н. П. Васильев, Е. В. Вельмякина, Д. В. Гуров, М. А. Иванов, И. В. Матвейчиков, Н. А. Мацук, Д. М. Михайлов, Л. И. Шустова; под ред. М. А. Иванова. – М.: НИЯУ МИФИ, 2011. – 328 с.

113. РД 03-418-01. Методические указания по проведению анализа риска опасных производственных объектов. – М.: Госгортехнадзор России. – 22 с.

114. Рогозин Е. А. Моделирование и алгоритмизация процесса проектирования программных систем защиты информации: дис. … докт. техн. наук: 05.13.12 / Е. А. Рогозин. – Воронеж: Воронежский государственный технический университет, 2006. – 307 с.

115. Росенко А. П. Внутренние угрозы безопасности конфиденциальной безопасности: Методология и теоретическое исследование. – М.: КРАСНАД, 2010. – 160 с.

116. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Гостехкомисиия России, 1992 г. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/296 (дата обращения 25.09.2017).

117. Руководящий документ. Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/314 (дата обращения 25.09.2017).

118. Руководящий документ. Безопасность информационных технологий. Руководство по формированию семейств профилей защиты. Гостехкомиссия России, 2003 г. [Электронный ресурс] URL: http://fstec.ru/en/component/attachments/download/312 (дата обращения 25.09.2017).

119. Руководящий документ. Временное положение по организации, разработки, изготовления и эксплуатации программных и технических средств защиты информациот несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Гостехкомисиия России, 1992 г. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/315 (дата обращения 25.09.2017).

120. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992 г. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/298 (дата обращения 25.12.2016).

121. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомисиия России, 1992 г. [Электронный ресурс] URL: http://fstec.ru/en/component/attachments/download/299 (дата обращения 25.09.2017).

122. Руководящий документ Руководство по разработке профилей защиты и заданий по безопасности. Гостехкомиссия России, 2003 г. [Электронный ресурс] URL: http://fstec.ru/en/component/attachments/download/311 (дата обращения 25.09.2017).

123. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомисиия России, 1992 г. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/297 (дата обращения 25.09.2017).

124. Румянцев П. В. Исследование механизма рандомизации распределения адресного пространства в операционной системе Windows Vista / П. В. Румянцев // Информационные системы и технологии. 2009. №4 (54). С. 24 – 31.

125. Саенко И. Б., Агеев С. А. Метод интеллектуального многоагентного управления рисками информационной безопасности в защищенных мультисервисных сетях специального назначения / И. Б. Саенко, С. А. Агеев // T-Comm: Телекоммуникации и транспорт. 2015. №1. С. 5 – 10.

126. Саенко И. Б., Кий А. В., Бушуев С. Н. Методика управления доступом к информационным ресурсам на основе анализа активности приложений. В сборнике: Наука сегодня: факты, тенденции, прогнозы. Материалы международной научно-практической конференции: в 2х частях. Научный центр «Диспут». 2016. С. 69 – 71.

127. Теория и практика обеспечения информационной безопасности / под ред. П. Д. Зегжды. – М.: Изд-во агентства «Яхтсмен», 1996. – 298 с.

128. Требования безопасности информации к операционным системам: утв. приказом директора ФСТЭК России от 26 августа 2016 г. №119. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/1051 (дата обращения 25.09.2017).

129. Требования к межсетевым экранам: утв. приказом директора ФСТЭК России от 9 февраля 2016 г. №9. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/913 (дата обращения 25.09.2017).

130. Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: утв. приказом директора ФСТЭК России от 11 марта 2014 г. №31. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/718 (дата обращения 25.09.2017).

131. Требования к системам обнаружения вторжений: утв. приказом директора ФСТЭК России от 6 февраля 2011 г. №638. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/305 (дата обращения 25.09.2017).

132. Требования к средствам антивирусной защиты: утв. приказом директора ФСТЭК России от 20 марта 2012 г. №28. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/402 (дата обращения 25.09.2017).

133. Требования к средствам доверенной загрузки: утв. приказом директора ФСТЭК России от 27 сентября 2013 г. №119. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/663 (дата обращения 25.09.2017).

134. Требования к средствам контроля съемных машинных носителей информации: утв. приказом директора ФСТЭК России от 5 сентября 2014 г. №87. [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/744 (дата обращения 25.09.2017).

135. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: утв. приказом директора ФСТЭК России от 11 февраля 2013 г. №17 (в редакции приказа ФСТЭК России от 15 февраля 2017 г. № 27). [Электронный ресурс] URL: http://fstec.ru/component/attachments/download/567 (дата обращения 25.09.2017).

136. Тутубалин П. И., Моисеев В. С. Вероятностные модели обеспечения информационной безопасности автоматизированных

систем обработки информации и управления. – Казань: РИЦ «Школа», 2008. – 144 с.: ил.

137. Федоров Ю. Н. Справочник инженера по АСУТП: Проектирование и разработка. Учебно-практическое пособие. – М.: Инфра-Инженерия, 2008. – 928 стр., 12 ил.

138. Хоффман Л. Дж. Современные методы защиты информации. – М.: Советское радио, 1980. – 264 с.

139. Чобанян В. А, Шахалов И. Ю. Анализ и синтез требований к системам безопасности объектов критической информационной инфраструктуры / В. А. Чобанян, И. Ю. Шахалов // Вопросы кибербезопасности. 2013. №1 (1). С. 17 – 27.

140. Щербаков А. Ю. Методы и модели проектирования средств обеспечения безопасности в распределенных компьютерных системах на основе создания изолированной программной среды: дис. … докт. техн. наук: 05.13.12, 05.13.13 / А. Ю. Щербаков. – М.: Московский государственный институт электроники и математики, 1997. – 320 с.

141. Язов Ю. К., Бурушкин А. А., Иванов С. М. Основные стратегии защиты информации в компьютерных системах / Ю. К. Язов, А. А. Бурушкин, С. М. Иванов // Информация и безопасность. 2008. №1. С. 118 – 121.

142. Язов Ю. К. Основы методологии количественной оценки эффективности защиты информации в компьютерных системах. – Ростов-на-Дону: СКНЦ ВШ, 2006. – 274 с.

143. Язов Ю. К., Соловьев С. В. Защита информации в информационных системах от несанкционированного доступа. – Воронеж.: Кварта, 2015. – 440 с.

Приложение А

Таблица А.1 – Виды и способы реализации основных компьютерных атак

№	Вид компьютерной атаки	Способ реализации компьютерной атаки	Угрозы, реализуемые компьютерной атакой
1	Анализ сетевого трафика	1.1 Анализ пакетов данных на канальном уровне	угрозы нарушения конфиденциальности информации; угрозы раскрытия особенностей построения АСУ.
		1.2 Анализ пакетов данных на сетевом уровне	
2	Сканирование сети	2.1 Сканирование пакетом TCP с флагом SYN	угрозы раскрытия особенностей построения АСУ.
		2.2 Сканирование пакетом TCP с флагом FIN	
		2.3 Сканирование пакетом TCP с флагом ACK	
		2.4 Сканирование пакетом TCP с флагом XMAS	
		2.5 Сканирование пакетом TCP с флагом NULL	
		2.6 Сканирование пакетом UDP	
		2.7 Сканирование пакетом ICMP	
3	Сканирование протоколов передачи сети	3.1 Сканирование по протоколу RIP	угрозы раскрытия особенностей построения АСУ.
		3.2 Сканирование по протоколу OSPF	
		3.3 Сканирование по протоколу SNMP	
		3.4 Сканирование по протоколу HTTP	
		3.5 Сканирование по протоколу SAMBA	
		3.6 Сканирование по протоколу TELNET	
		3.7 Сканирование по протоколу POP3	
		3.8 Сканирование по протоколу NNTP	
		3.9 Сканирование по протоколу FINGER	
		3.10 Сканирование по протоколу FTP	
		3.11 Сканирование по протоколу TFTP	
		3.12 Сканирование по протоколу RLOGIN	

№	Вид компьютерной атаки	Способ реализации компьютерной атаки	Угрозы, реализуемые компьютерной атакой
		3.13 Сканирование по протоколу IDENT	
		3.14 Сканирование по протоколу IMAP	
		3.15 Сканирование по протоколу RPC	
		3.16 Сканирование по протоколу Modbus/TCP (или по другим промышленным протоколам)	
4	Локальное проникновение в критически важный сегмент АСУ	4.1 Ransomware	угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации; угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования; угрозы раскрытия особенностей построения АСУ.
		4.2 Toolkit	
		4.3 Badware	
		4.4 Rootkit	
		4.5 Trojan	
		4.6 Spyware	
5	Удаленное проникновение в критически важный сегмент АСУ	5.1 Backdoor	угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации; угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования; угрозы раскрытия особенностей построения АСУ.
		5.2 XML-бомба	
		5.3 Средства удаленного администрирования	
		5.4 Phishing	
		5.5 Атаки «нулевого дня»	
		5.6 Browser hijackers	
6	Взлом паролей	6.1 Изменения системных файлов	угрозы нарушения конфиденциальности информации; угрозы нарушения целостности информации; угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования; угрозы раскрытия особенностей построения АСУ.
		6.2 Программные закладки	
		6.3 Перебор данных в системных файлах	
		6.4 Программа сброса паролей	
		6.5 Программа взлома паролей	
7	Ввод ложной информации	7.1 Программные закладки	угрозы нарушения целостности информации; угрозы нарушения штатного режима функционирования.
		7.2 Средства удаленного администрирования	
8	Разрушение	8.1 Trojan	угрозы нарушения

№	Вид компьютерной атаки	Способ реализации компьютерной атаки	Угрозы, реализуемые компьютерной атакой
	информации и программного обеспечения	8.2 Rootkit 8.3 Программные закладки 8.4 Средства удаленного администрирования	целостности информации; угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования.
9	Локальный отказ в обслуживании	9.1 «Тяжелый пакет» 9.2 MAC-flooding	угрозы нарушения доступности информации; угрозы нарушения правильности функционирования; угрозы нарушения штатного режима функционирования.
10	Удаленный отказ в обслуживании	10.1 Smurf 10.2 Fraggle 10.3 SYN-flooding	угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования.
11	Логическое отключение абонентов	11.1 Перехват IP-адреса	угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования.
12	Логическая подмена сервера	12.1 Запросы по протоколу RIP 12.2 Запросы по протоколу OSPF	угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования.
13	Перенаправление пакетов данных	14.1 Запросы по протоколу SNMP 13.2 Запросы по протоколу ICMP 13.3 Запросы по протоколу SAP 13.4 Запросы по протоколу ARP 13.5 Запросы по протоколу DNS 13.6 Передача заранее подготовленного ложного ответа	угрозы нарушения доступности информации; угрозы нарушения штатного режима функционирования.

Приложение Б

Таблица Б.1 – Пример множества функций для средств антивирусной защиты

Номер функции	Содержание функции, реализуемой средством антивирусной защиты
1	Сигнатурный поиск по коду
1.1	– обеспечивается возможность выполнения проверок с целью обнаружения вредоносных программ в файловых областях носителей информации, системных областях операционной системы на носителях информации, а также в оперативной памяти
1.2	– проверки с целью обнаружения вредоносных программ производятся по команде, с предварительным заданием объекта или области проверки, а также путем постоянного мониторинга объектов файловой системы, системных областей операционной системы, а также оперативной памяти
2	Сигнатурный поиск по событиям
2.1	– обеспечивается возможность выполнения проверок с целью обнаружения вредоносных программ в файловых областях носителей информации, системных областях операционной системы на носителях информации, а также в оперативной памяти
2.2	– проверки с целью обнаружения вредоносных программ путем постоянного мониторинга объектов файловой системы, системных областей операционной системы, а также оперативной памяти
3	Эвристический поиск по коду
3.1	– обеспечивается возможность выполнения проверок с целью обнаружения вредоносных программ в файловых областях носителей информации, системных областях операционной системы на носителях информации, а также в оперативной памяти
3.2	– проверки с целью обнаружения вредоносных программ производятся по команде, с предварительным заданием объекта или области проверки, а также путем постоянного мониторинга объектов файловой системы, системных областей операционной системы, а также оперативной памяти
4	Эвристический поиск по событиям
4.1	– обеспечивается возможность выполнения проверок с целью обнаружения вредоносных программ в файловых областях носителей информации, системных областях операционной системы на носителях информации, а также в оперативной памяти
4.2	– проверки с целью обнаружения вредоносных программ путем постоянного мониторинга объектов файловой системы, системных областей операционной системы, а также оперативной памяти
5	Обновление баз сигнатур
5.1	– обеспечивается локальное обновление баз сигнатур без применения средств автоматизации
6	Обновление баз эвристических правил
6.1	– обеспечивается локальное обновление баз эвристических правил без применения средств автоматизации
7	Аудит событий

Номер функции	Содержание функции, реализуемой средством антивирусной защиты
7.1	– обеспечивается возможность генерирования записей аудита для следующих событий: запуск средства антивирусной защиты; запуск проверки; окончание проверки; запуск обновления базы сигнатур; окончание обновления базы сигнатур; запуск обновления базы эвристических правил; окончание обновления базы эвристических правил; обнаружение вредоносного объекта; действия, произведенные с вредоносным объектом; изменение режимов работы и параметров средства антивирусной защиты
7.2	– обеспечивается возможность чтения информации из записей аудита
7.3	– обеспечивается ограничение доступа к чтению записей аудита
7.4	– обеспечивается поиск, сортировка и упорядочение данных аудита
8	Управление режимами и параметрами
8.1	– обеспечивается возможность уполномоченным пользователям управлять режимом выполнения функций безопасности
8.2	– обеспечивается возможность уполномоченным пользователям управлять параметрами настройки функций безопасности

Приложение В

Пример формирования функциональных требований к средствам резервного копирования информации для четырех уровней реализации

1 уровень реализации функциональных требований (базовый):

1. Резервное копирование информации:

– должно быть обеспечено резервное копирование информации на резервные машинные носители информации с установленной периодичностью.

2. Обеспечение возможности восстановления информации из резервных копий:

– должно быть обеспечено восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного интервала.

2 уровень реализации функциональных требований (расширенный 1):

1. Резервное копирование информации:

– должно быть обеспечено резервное копирование информации на резервные машинные носители информации с установленной периодичностью;

– должна быть обеспечена регистрация событий, связанных с резервным копированием информации.

2. Обеспечение возможности восстановления информации из резервных копий:

– должно быть обеспечено восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного интервала;

– должна быть обеспечена регистрация событий, связанных с восстановлением данных.

3 уровень реализации функциональных требований (расширенный 2):

1. Резервное копирование информации:

– должно быть обеспечено резервное копирование информации на резервные машинные носители информации с установленной периодичностью;

– должна быть обеспечена регистрация событий, связанных с резервным копированием информации;

– должен быть обеспечен контроль целостности резервных копий по именам и атрибутам файлов резервных копий.

2. Обеспечение возможности восстановления информации из резервных копий:

– должно быть обеспечено восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного интервала;

– должна быть обеспечена регистрация событий, связанных с восстановлением данных.

4 уровень реализации функциональных требований (расширенный 3):

1. Резервное копирование информации:

– должно быть обеспечено резервное копирование информации на резервные машинные носители информации с установленной периодичностью;

– должна быть обеспечена регистрация событий, связанных с резервным копированием информации;

– должен быть обеспечен контроль целостности резервных копий, по контрольным суммам файлов резервных копий.

2. Обеспечение возможности восстановления информации из резервных копий:

– должно быть обеспечено восстановление информации с резервных машинных носителей информации (резервных копий) в течение установленного интервала;

– должна быть обеспечена регистрация событий, связанных с восстановлением данных.

Приложение Г

Пример тестовой процедуры по имитации компьютерной атаки вида «Локальный отказ в обслуживании»

Компьютерная атака «Локальный отказ в обслуживании». Данная атака преследует следующие цели: существенное снижение функциональных возможностей процесса, исчерпание места на диске и истощение индексных узлов. Профиль атаки «Локальный отказ в обслуживании» включает в себя (рисунок Г.1):

– начало атаки (*Start*);
– внедрение вредоносного кода (1);
– запуск вредоносного кода (2)
– формирование потока запросов обращения к файловой системе (3.1);
– генерация дополнительных потоков собственного процесса (3.2);
– генерация процессов с повторяющейся структурой (3.3);
– формирование потока регистрируемых в системных журналах событий (3.4);
– формирование потока запросов на создание файлов (3.5);
– конец атаки (*End*).

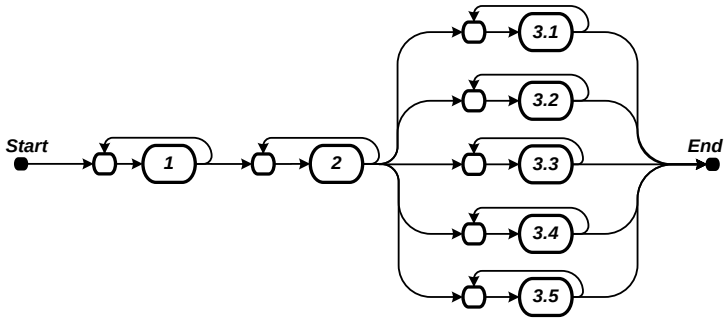


Рисунок Г.1 – Схема профиля компьютерной атаки «Локальный отказ в обслуживании»

Средства реализации данного типа компьютерной атаки пакет «Metasploit Framework» и программный комплекс анализа защищенности «Сканер-ВС».

Приложение Д

Пример тестовой процедуры для проверки наличия и корректности реализации меры защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей»

Для описания тестовой процедуры для проверки корректности реализации данной меры защиты введем следующие обозначения:

– N_{RAM} – число областей оперативной памяти, подлежащих проверке;

– N_{HDD} – число областей (файлов) на внешних накопителях информации, подлежащих проверке;

– $A_{RAM} = \left\{a_{RAM_1};\ a_{RAM_1}; \dots; a_{RAM_{N_{RAM}}}\right\}$ – множество областей оперативной памяти;

– $A_{HDD} = \left\{a_{HDD_1};\ a_{HDD_1}; \dots; a_{HDD_{N_{HDD}}}\right\}$ – множество областей на внешних накопителях;

– $S_{RAM} = \left\{s_{RAM_1};\ s_{RAM_1}; \dots; s_{RAM_{N_{RAM}}}\right\}$ – множество тестовых (проверочных) последовательностей символов для проверки очистки областей оперативной памяти.

– $S_{HDD} = \left\{s_{HDD_1};\ s_{HDD_1}; \dots; s_{HDD_{N_{HDD}}}\right\}$ – множество тестовых (проверочных) последовательностей символов для проверки очистки областей на внешних накопителях.

Последовательность действий при выполнении данной тестовой процедуры следующая:

1. Формирование множеств последовательностей символов S_{RAM} и S_{HDD}.

2. Определение числа областей оперативной памяти для проверки N_{RAM}.

3. Определение адреса начала и длины каждой области оперативной памяти для проверки.

4. Выделение выбранных областей A_{RAM} в оперативной памяти.

5. Заполнение выбранных областей оперативной памяти тестовыми последовательностями символов из множества S_{RAM}.

6. Освобождение (перераспределение) выбранных участков оперативной памяти.

7. Проверка наличия в областях оперативной памяти A_{RAM} тестовых последовательностей из множества S_{RAM}.

8. Принятие решения о корректности реализации меры защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» в части касающейся очистки оперативной памяти.

9. Определение числа областей на внешних накопителях информации для проверки N_{HDD}.

10. Определение характеристик областей на внешних накопителях информации (длина файла) для проверки.

11. Запись в выбранные области на внешних носителях тестовых последовательностей символов из множества S_{HDD}.

12. Очистка выбранных областей на внешних носителях информации (удаление файлов с записанными в них тестовыми последовательностями символов из множества S_{HDD}).

13. Поиск последовательностей символов из множества S_{HDD} по всему внешнему накопителю информации.

14. Принятие решение о корректности реализации меры защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» в части касающейся очистки внешних накопителей информации.

15. Принятие решения о корректности реализации меры защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» в целом.

Мера защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» в части касающейся очистки оперативной памяти считается реализованной корректно в случае, если по итогам проверки наличия в областях оперативной памяти A_{RAM} тестовых последовательностей из множества S_{RAM} (шаг 7) ни в одной из областей оперативной памяти из множества A_{RAM} не было обнаружено тестовых последовательностей из множества S_{RAM}.

Мера защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» в части касающейся очистки внешних носителей информации считается реализованной корректно в случае, если по итогам проверки наличия тестовых последовательностей из множества S_{HDD} по всему внешнему накопителю (шаг 13) не было

обнаружено ни одной тестовой последовательности из множества S_{HDD}.

Мера защиты «Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей» считается реализованной корректно в целом, если данная мера защиты в части касающейся очистки оперативной памяти и в части касающейся очистки внешних накопителей информации реализованы корректно.

Научное издание

Дроботун Евгений Борисович

Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления

Монография

Издательство «Наукоемкие технологии»
ООО «Корпорация «Интел групп»
197372, Санкт-Петербург, пр. Богатырский,
дом 32, к. 1 лит. А, пом. 6Н.
www.publishing.intelgr.com
Тел.: +7 (812) 945-50-63
E-mail: publishing@intelgr.com

Отпечатано: Цифровая типография «Принт-Копи»,
170024, г. Тверь, пр. Ленина, 18/1.
www.print-copy.ru, www.принт-копи.рф
Тел./факс: 8(4822) 44-57-08, моб.: 8-904-355-30-10
E-mail: 445708@mail.ru

ISBN 978-5-9909412-2-9

Гарнитура «TimesNewRoman». 7,5 усл.п.л.
Тираж 500 экз. Подписано в печать 12.10.2017. Заказ №15

Материалы изданы в авторской редакции