

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 100502 –

Специализация -

Информационная безопасность
телекоммуникационных систем
Разработка защищенных
телекоммуникационных систем

ДИПЛОМНАЯ РАБОТА

на тему

ИММУНОЛОГИЧЕСКИЕ СИСТЕМЫ В ОБЕСПЕЧЕНИИ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Студент	_____	<u>Никулина Ирина Александровна</u>
Руководитель	_____	<u>Сулов В.А.</u>
Нормоконтролёр	_____	<u>Фатеев А.Г.</u>
Рецензент зам. начальника отделения АО «ПНИЭИ»	_____	<u>Сомкин С.А.</u>

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефилов

Работа защищена с отметкой _____ (протокол заседания ГЭК
от _____ № _____)

Секретарь ГЭК _____ А.Г. Фатеев

Пенза 2016

РЕФЕРАТ

Отчет содержит 66 с., 16 рис., 1 табл., 11 источников, 2 приложения.

ИММУНОЛОГИЧЕСКАЯ СИСТЕМА, СИСТЕМА ОБНАРУЖЕНИЯ НАРУШЕНИЙ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, АЛГОРИТМ ОТРИЦАТЕЛЬНОГО ОТБОРА, ДВОЙНАЯ ПЛАСТИЧНОСТЬ, ИММУННЫЙ ОТВЕТ

Данная дипломная работа посвящена направлению исследования искусственных иммунологических систем.

Целью дипломной работы является исследование возможностей создания иммунологических систем в информационной безопасности и способов выявления нарушений.

Предметом исследования являются процессы проектирования и использования искусственных иммунологических систем.

В результате дипломной работы были созданы: функциональная модель иммунологической системы, модель принципа действия иммунологической системы, структурная модель иммунологической системы и изучены теоретические аспекты исследования иммунологических систем в информационной безопасности.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ
Федеральное государственное бюджетное образовательное учреждение
высшего образования

ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УДК 004.056

Политехнический институт

УТВЕРЖДАЮ

Факультет приборостроения,
информационных технологий и
электроники
Выпускающая кафедра:
Информационная безопасность систем
и технологий
Учебная группа 11ПТ1

Зав. кафедрой ИБСТ
к.т.н., доцент С.Л. Зефилов

« 6 » 10 2016 г.

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ
НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ
РАБОТУ**

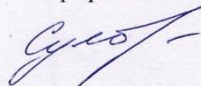
студента группы 11ПТ1 Никулиной Ирины Александровны

Специальность 100502 – Информационная безопасность
телекоммуникационных систем

Тема дипломной работы:

Иммунологические системы в обеспечении информационной безопасности

Руководитель ВКР
инженер НИОИ-9, ПНИЭИ



В.А. Сулов

Нормоконтролер
к.т.н., доцент кафедры ИБСТ



А.Г. Фатеев



1 Цели и задачи ВКР

Цель работы – исследование возможностей создания иммунологических систем в информационной безопасности и способов выявления нарушений.

В данном исследовании проводится моделирование иммунологических систем с целью их изучения и применения в обеспечении информационной безопасности.

2 Тактико – технические требования к выполнению ВКР

Создать модели системы:

- функциональную модель, предназначенную для изучения особенностей работы;
- модель принципа действия, характеризующую существенные связи и свойства, обеспечивающие функционирование системы;
- структурную модель, характеризующую последовательность и состав стадий и этапов работы.

Должны удовлетворяться следующие требования к моделям систем:

- универсальность, т.е. применимость к ряду однотипных систем в нескольких режимах функционирования;
- точность, т.е. степень совпадения полученных в процессе моделирования результатов с заранее установленными.

В ВКР должны быть рассмотрены следующие вопросы:

- обзор возможностей создания моделей иммунных систем информационной безопасности;
- обзор регулирования взаимоотношений защищенной системы с внешней средой;
- способы выявления нарушений информационной безопасности и определение мер реагирования на нарушения;
- обзор состояния и тенденций развития данного направления в информационной безопасности;
- основные области применения иммунологического подхода.

3 Требования к разрабатываемой документации

Отчет по ВКР выполняется в соответствии с требованиями ГОСТ 7.32.

Перечень и содержание графической части ВКР:

- структура иммунологической системы – 1 л., ф. А1 (плакат);
- структура антивирусной защиты на базе иммунологических принципов – 1 л., ф. А1 (плакат);
- структура аутентификации с использованием обновляемого множества наборов – 1 л., ф. А1 (плакат);
- функциональная модель иммунологической системы – 1 л., ф. А1 (плакат);
- выявление нарушений и меры реагирования – 1 л., ф. А1 (плакат);
- области применения иммунологического подхода – 1 л., ф. А1 (плакат).

Электронная копия отчета и графической части ВКР должна быть представлена на магнитном или оптическом носителе.

4 Сроки выполнения ВКР

Тема утверждена приказом ректора ПГУ № ____ от «__» ____ 2016 г.

Дата выдачи задания «6» 09 2016 г.

Время дипломного проектирования с ____ 2016 г. по ____ 2016 г.

Задание к исполнению принял «__» ____ 2016 г.

Исполнитель ВКР Никulina И.А. Никulina И.А.

СОДЕРЖАНИЕ

Введение.....	9
1 Теоретические аспекты исследования иммунологических систем в информационной безопасности	12
1.1 Предпосылки и возможности создания моделей иммунных систем в информационной безопасности	12
1.2 Обзор регулирования взаимоотношений защищенной системы с внешней средой	20
1.3 Способы выявления нарушений информационной безопасности и определение мер реагирования на нарушения	25
1.4 Состояние и тенденции развития иммунологического подхода в информационной безопасности	29
1.5 Основные области применения иммунологического подхода.....	33
1.5.1 Применение иммунологического подхода	33
1.5.2 Средство сетевой самозащиты.....	34
1.5.3 Средство антивирусной защиты	37
1.5.4 Средство аутентификации.....	42
1.5.5 Средство клавиатурного мониторинга	44
1.5.6 Система активного аудита.....	46
2 Комплекс моделей иммунологических систем	50
2.1 Функциональная модель иммунологической системы	50
2.2 Модель принципа действия иммунологической системы	55
2.3 Структурная модель иммунологической системы	57
Заключение	59
Список использованных источников	60
ПРИЛОЖЕНИЕ А Анкеты, заполненные экспертами по информационной безопасности	62
ПРИЛОЖЕНИЕ Б Проверка ВКР на оригинальность	Ошибка! Закладка не определена

ОПРЕДЕЛЕНИЯ

В данной дипломной работе применяются термины с соответствующими определениями:

Искусственная иммунологическая система – адаптивная вычислительная система, использующая модели, принципы, механизмы и функции, описанные в теоретической иммунологии, которые применяются для решения прикладных задач [10].

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АОО – алгоритм отрицательного отбора;

БД – база данных;

ВКР – выпускная квалификационная работа;

ИИС – искусственная иммунологическая система;

ИС – информационная система;

ИТ – информационные технологии;

КМ – клавиатурный мониторинг;

НСД – несанкционированный доступ;

ОС – операционная система;

ПО – программное обеспечение;

СЗИ – средство защиты информации.

ВВЕДЕНИЕ

В современном мире информация стоит на первом месте, являясь самым востребованным ресурсом. Потеря или нежелательная модификация информации в большинстве случаев может привести к значительному ущербу. Основная задача в обеспечении безопасности информации – это построение системы защиты информации. Самой главной проблемой при создании системы защиты информации является проблема постоянного возникновения новых, ранее не выявленных угроз. Для эффективной работы система информационной безопасности должна обладать свойством самообучения, иметь механизмы генерации новых правил информационной безопасности. Также одной из самых важных характеристик системы защиты информации является такое свойство как адаптивность, так как адаптивная система сохраняет работоспособность при любых изменениях свойств объекта или окружающей среды путем смены алгоритма своего функционирования.

Принципы работы и механизмы иммунологической системы используются для построения алгоритмов анализа данных, оптимизации и распознавания систем информационной безопасности.

Данная дипломная работа посвящена такому направлению, как искусственные иммунологические системы.

Целью дипломной работы является исследование возможностей создания иммунологических систем в информационной безопасности и способов выявления нарушений.

Предметом исследования являются проектирование и использование искусственных иммунологических систем в обеспечении информационной безопасности.

В данном исследовании проводится моделирование иммунологических систем с целью их изучения и применения в обеспечении информационной безопасности.

Актуальность данной темы обусловлена необходимостью автоматизации процесса реагирования системы безопасности информации на нарушения, атаки во время функционирования, а также ростом атак на информационные системы, что влечёт за собой целый ряд различного рода убытков.

В первой главе дипломной работы был произведен обзор теоретических аспектов исследования иммунологических систем в обеспечении информационной безопасности. Были исследованы предпосылки и возможности создания моделей иммунных систем в информационной безопасности, регулирование взаимоотношений защищенной системы с внешней средой, способы выявления нарушений информационной безопасности и определение мер реагирования на нарушения, состояние и тенденции развития иммунологического подхода в информационной безопасности, основные области применения иммунологического подхода.

Во второй главе был создан комплекс моделей иммунологических систем, включающий в себя:

- функциональную модель;
- модель принципа действия;
- структурную модель.

В ходе ВКР были получены следующие результаты:

- разработана и описана структурная модель иммунологической системы;
- разработана и описана модель принципа действия иммунологической системы;
- разработана и описана функциональная модель иммунологической системы;
- предложен алгоритм подавления нарушений на основе алгоритма отрицательного отбора;

– приведены возможные области применения иммунологического подхода в области информационной безопасности.

1 Теоретические аспекты исследования иммунологических систем в информационной безопасности

1.1 Предпосылки и возможности создания моделей иммунных систем в информационной безопасности

Современные СЗИ не полностью справляются со стоящими перед ними задачами: обнаружение нарушений, поддержание приемлемого уровня защиты. Защита от вредоносного ПО в большинстве случаев реализуется за счёт использования специального антивирусного ПО, осуществляющего проверку компонентов компьютерной системы на наличие изученных ранее сигнатур вредоносного ПО. Базы сигнатур обновляются производителем антивирусного ПО и поставляются пользователям, осуществившим подписку. В большинстве случаев подписка на получение обновлений антивирусного ПО является платной, так как требует от производителей такого ПО затрат на поиск и извлечение сигнатур всё новых и новых вредоносных программ, появляющихся каждый день. Но даже частые обновления баз не могут полностью обезопасить систему при встрече с новым вредоносным ПО, неизвестным ранее производителям антивирусного ПО.

Большинство технологий и методов защиты информации изначально заимствованы из механизмов, рассмотренных человеком в живой природе. Многие из этих механизмов также являются прямым отражением механизмов организации человеческого общества. Вредоносные программы являются аналогами вирусов, от которых и получили своё общепринятое название, их аналогами в человеческом обществе являются преступники. Природные механизмы весьма сложны за счёт неоднородности живой природы и не все из них до конца изучены, их аналоги в информационной сфере гораздо примитивнее. При рассмотрении и использовании сути природных механизмов не требуется их абсолютное осознание, достаточно близкой модели. Важным является рассмотрение защитных механизмов, которые живые организмы применяют для поддержания жизни в опасных условиях

внешней среды. В таких условиях живые организмы были вынуждены найти лучшие из возможных способов защиты на всех уровнях жизнедеятельности. К примеру, механизмы иммунитета, созданные в процессе эволюции, позволяют уничтожать вредоносные клетки внутри организма, а также части самого организма, утратившие возможность правильно функционировать. При этом практически все живые организмы имеют возможности обнаружения вредных воздействий и регенерации при необратимых повреждениях части организма, позволяя частично или полностью восстановить его функциональность, восстановив или заменив разрушенные ткани.

Рассматривая механизмы иммунитета, можно заметить, что существует чёткая специализация иммунных клеток – некоторые из них позволяют обнаружить место проявления проблемы, другие блокируют повреждённые участки, позволяя локализовать последствия, отдельные клетки специализируются на выявлении и маркировке чужих объектов, нестандартно функционирующих собственных клеток, существуют специализированные уничтожители маркированных объектов, а также очищающие клетки, которые удаляют последствия уничтожения инородных объектов и т.д.

Основной вопрос в обеспечении ИБ – это создание системы защиты информации, при котором главной проблемой является непрерывное появление новых, ранее неизведанных угроз. Поэтому для эффективной работы система защиты информации должна уметь обучаться и сама вырабатывать меры борьбы и защиты. Такая системы защиты информации должна быть саморазвивающейся, она могла бы самостоятельно реагировать на угрозы ИБ. Также система защиты информации должна быть адаптивной системой, сохраняющей работоспособность при любых изменениях внутренней или внешней среды. Принцип работы таких систем заключается в применении иммунной системы человека. Иммунная система человека обеспечивает защиту его организма от азличных угроз и представляет собой

сложную адаптивную систему. Главной задачей иммунной системы является принцип разделения их на «своих» и «чужих».

При обнаружении чужеродных клеток активируются защитные механизмы организма человека. В дальнейшем происходит распознавание данной угрозы, после чего формируется память к ней, чтобы в дальнейшем при встрече такой же угрозы незамедлительно противодействовать ей. Принципы ИИС активно используются при решении задач, связанных с ИБ, например:

- обнаружение компьютерных вирусов;
- организация парольной защиты;
- мониторинг процессов в системе UNIX и др.

ИИС необходима для автоматизации процесса реагирования системы на внешние и внутренние нарушения функционирования.

В сфере ИБ ИИС могут решать следующие задачи:

- противодействие распространению вредоносной активности;
- выявление неавторизованного использования информационных ресурсов;
- обнаружение нарушений в ИС;
- обнаружение аномалий в информационных процессах;
- сохранение целостности информации;
- управление инцидентами ИБ и др.

Большинство из перечисленных выше задач сводится к проблеме нахождения отличий «своего» от потенциально опасного «чужого».

Иммунологический подход позволяет системам обучаться во время функционирования, самостоятельно обнаруживать нарушения и самостоятельно вырабатывать способы борьбы с ними. Вследствие способности к дообучению во время функционирования, ИИС относятся к системам искусственного интеллекта, которые находят все большее применение в системах защиты информации.

Распознавание образов осуществляется централизованно, на системном уровне с применением различных методов сопоставления неизвестных образцов с эталонными образцами, используя при этом следующие методы:

- геометрические;
- параметрические;
- статистические;
- аппарат искусственных нейронных сетей и др.

Принятие решения о том к какому классу отнести неизвестный образец осуществляется по окончании всего цикла сопоставления образцов, что во многих случаях может оказаться уже запоздалой реакцией.

К наиболее развитым ИТ, пригодным для решения задач ИБ, можно отнести искусственные нейронные сети и генетические алгоритмы, а к наиболее перспективным - искусственные иммунные системы и иммунокомпьютинг.

Иммунная система живого организма осуществляет регулирование его взаимоотношений с внешней средой в сфере микробиологической безопасности, с её помощью организм человека противодействует чужеродным клеткам. Основное свойство иммунной системы человека – выявление антигенов и активация иммунного ответа. Ключевым механизмом появления такой способности является отрицательный отбор – сложный физико-химический процесс распознавания антигенов. При обнаружении «чужих» включаются механизмы нейтрализации и разрушения антигенов [1].

Иммунная система способна эффективно обрабатывать значительные объемы данных. Исследование иммунных систем в области информатизации, в том числе в области ИБ, привело к появлению искусственных иммунологических систем. В отличие от информационных систем ИИС выполняют полностью децентрализованную обработку, в том числе и при решении задач распознавания [1].

Можно заметить аналогию функций естественной иммунной системы с основными функциями, которые должна выполнять система управления инцидентами ИБ:

- выявление, регистрация, оценка событий, которые предположительно являются инцидентами, сбор доказательств для дальнейшего расследования;
- идентификация инцидента, принятие решения в условиях полной неопределенности имеющейся информации и при необходимости оповещение об инциденте;
- устранение последствий инцидента с помощью ресурсов безопасности.

Аналогия иммунной системы с информационной системой приведена на рисунке 1.

Иммунная система	Компьютерная имплементация
Отрицательный отбор Т-лимфоцитов	Алгоритм отрицательного отбора
Клональная селекция В-лимфоцитов	Алгоритм клональной селекции
Иммунная сеть	Формальная иммунная сеть (FIN, Formal Immune Network)

Рисунок 1- Аналогия иммунной системы человека с информационной системой

Самой распространенной моделью ИИС, применяемой в области ИБ является АОО.

Одной из необходимых составляющих адаптивных систем защиты являются подсистемы мониторинга и активного аудита, с помощью которых осуществляется сбор статистических данных о событиях в системе, ключевых параметров функционирования системы и сделать вывод о

нарушениях в работе, возможных аномалий, которые происходят в системе и отличия текущего уровня безопасности с допустимым.

Обнаружения атак и аномалий в состоянии системы является процессом обнаружения отклонений от эталона состояния системы.

ИИС активно применяются в следующих областях:

- принятие решений;
- управление ИБ;
- диагностика атак;
- диагностика аномальных состояний;
- распознавание образов и др.

Построение ИИС основывается на иммунной системе человека, преимуществом которых является возможность получения противодействия к неизвестным угрозам, что позволит существенно повысить адаптивность механизмов и функций подсистем защиты информации и справиться с проблемами средств обеспечения ИБ.

Изначально ИИС необходим временной период, во время которого система проходит обучение, формирование базы знаний. Для каждого состояния функционирования системы строится интервал допустимых значений, в пределах которого допустимо отклонение. Затем, во время функционирования ИИС оценивает отклонения текущих значений от значений, полученных в период обучения, принятые за эталон. Если отклонения выходят за рамки допустимого интервала, то фиксируется наличие аномалии, атаки. Для статистического анализа характерен высокий уровень ложных срабатываний при использовании в локальных сетях.

Иммунный ответ является первым этапом борьбы с вредоносной активностью, который запускается сразу же после его реализации и заключается в локализации места воздействия вредоносного фактора на элементы системы защиты информации с целью предотвращения

дельнейшего нарушения процесса функционирования подсистем защиты информации и системы в целом.

Защитный механизм системы защиты информации включает в себя следующие этапы:

- определение места отказа ресурса, т. е. слабое место, в котором была реализована атака;
- снятие с данного ресурса системных процессов;
- перенаправление системных задач на другой ресурс;
- исключение отказавшего ресурса из конфигурации системы защиты информации;
- прекращение взаимосвязи с отказавшим ресурсом и запрет доступа к нему;
- попытка восстановления отказавшего ресурса.

Если сравнивать ИИС с иммунной системой человека, то необходимо учитывать, что применение ИИС в ИБ должно носить многообразный характер.

Существующие системы обнаружения аномалий обладают рядом недостатков, которые не позволяют их широко использовать в корпоративных сетях, это объясняется сложностью их реализации, включающей в себя:

- выбор методики сбора данных об ИС;
- выбор способа противодействия атаке;
- обработку входных данных;
- выбор метода обнаружения атак;
- распределение нагрузки на компоненты ИС.

Уже исследованные методы обнаружения атак, такие, как метод обнаружения аномалий и сигнатурный метод, не позволяют достичь нужного эффекта обнаружения атак. Нейросетевые методы обнаружения атак

позволяют достичь приемлемых характеристик, но обладают следующими недостатками:

- трудность выбора параметров;
- трудность выбора структуры нейронных сетей;
- ресурсоемкий характер обучения нейронной сети;
- сложность дообучения и переобучения нейронной сети.

Возникает необходимость в выборе и применении такого метода, с помощью которого стало бы возможным избежать указанных выше недостатков при необходимом уровне надежности обнаружения атак. Перспективным направлением является построение систем на основе технологий ИИС. Данный метод обладает рядом преимуществ по сравнению с другими методами, обеспечивая:

- высокую скорость работы;
- сравнительно простой алгоритм обучения;
- низкую ресурсоемкость.

Режим функционирования ИИС – непрерывный системный процесс проверки ИС на соответствие декларируемым целям политики безопасности, организации обработки данных, норм эксплуатации средств вычислительной техники, а также автоматического реагирования на выявленные отклонения.

Выделяя иммунологические системы, можно сказать, что их существенное преимущество перед генетическими алгоритмами и искусственными нейронными сетями – это способность к обучению и наличие памяти.

Из вышесказанного можно сделать вывод о том, что исследование искусственных иммунологических систем является весьма перспективным направлением в обеспечении информационной безопасности.

1.2 Обзор регулирования взаимоотношений защищенной системы с внешней средой

Основная задача системы информационной безопасности – это обеспечение защиты информации и постоянное функционирование информационной системы с соблюдением следующих свойств информации:

- конфиденциальность информации (обнаружение возможных источников утечки информации; предотвращение НСД к информации);
- целостность информации (предотвращение несанкционированного изменения информации);
- доступность информации (предотвращение несанкционированного ограничения доступа к информации).

Система информационной безопасности уже заведомо функционирует в опасной внешней среде. Регулирование взаимоотношений защищенной системы с внешней средой определяется принятой политикой безопасности. В случае обнаружения нарушения информационной безопасности система защиты информации принимает определенные меры реагирования.

Большая часть задач системы информационной безопасности сводится к проблеме нахождения отличий «своего» (пользователей, которые обладают определенными полномочиями, допустимых процессов, допустимого программного кода и др.) от потенциально опасного «чужого» (пользователей, которые не обладают определенными полномочиями и недопустимых процессов, испорченных данных, зловредного программного кода) [3].

Регулирование взаимоотношений организма с внешней средой в сфере микробиологической безопасности называется иммунным ответом, суть которого заключается в нейтрализации или уничтожении вредоносных клеток. Данное решение принимается совместными действиями клеток иммунной системы самостоятельно, без задействования нервной системы организма (верхних уровней иерархии) [3].

Ключевым свойством ИИС, не нашедшим отражения в АОО, является их двойная внутренняя пластичность. Двойная пластичность обеспечивает функционирование иммунологической системы в условиях непрерывных возмущений, вызываемых онтогенетическими изменениями организма и его взаимодействием с внешней средой. Двойная пластичность отражает способность ИИС к адаптации на основе параметрических и структурных изменений. Термином «параметрическая пластичность» обозначают механизм адаптации, позволяющий системе в ходе выполнения некоторой задачи изменять параметры функционирования для повышения ее эффективности [9].

С помощью двойной пластичности обеспечивается функционирование ИИС в условиях непрерывных возмущений, вызываемых онтогенезом и внешней средой. Структурная пластичность дает системе новые возможности для адаптации. В системах взаимодействующих элементов структурная пластичность сводится к способности добавления новых элементов и исключения уже имеющихся элементов.

Структурные изменения (приток новых антител) происходят реже, чем параметрические изменения (изменение концентрации антител).

Структурные изменения зависят от временной эволюции параметров системы. Приток антител второго типа происходит лишь после того, как концентрация антител первого типа достигает определенного уровня. Характер структурных изменений определяется системными взаимодействиями, а не только внешними факторами. Вновь добавляемые элементы комплементарны, а не подобны уже имеющимся.

Из рассмотрения модели функционирования ИИС можно сделать следующий вывод: достижение полезного результата достигается за счёт совместного поведения системы, а не ее взаимодействие с внешней средой [5].

Именно это даёт возможность использовать иммунологический подход, важные свойства ИИС в моделях систем информационной безопасности для

применения свойств адаптивности в условиях высокой динамики взаимодействия с потенциально опасной внешней средой.

Свойство двойной пластичности ИИС позволяет сформулировать основные принципы параметрической и структурной адаптации при их моделировании в системах информационной безопасности:

- структурные изменения должны определяться динамикой изменения параметров системы, обусловленных внутрисистемными процессами, и не зависеть от внешних факторов;
- масштаб времени структурной адаптации должен быть больше масштаба времени параметрической адаптации;
- структурные изменения должны отражаться в количественных характеристиках системы, отражающих совместные действия элементов.

АОО, отражающий две стадии пластичности, свойственные ИИС, в упрощенном виде выглядит следующим образом:

- первоначальная конфигурация системы безопасности информации, как модели ИИС, создается на основе АОО, после чего она включается в режим функционирования;
- в процессе функционирования системы безопасности информации будут возникать события, состоящие в появлении строк входного сигнала, отмеченных в памяти системы как «чужие» (антиген), эти события вызовут активирование определенных детекторов (антитела);
- активировавшиеся детекторы размножаются с сохранением аффинности со строками входного сигнала, вызвавшими их срабатывание.

Приведен следующий пример.

На вход системы поступил сигнал, содержащий сочетание значений

10 30 21,

которое привело к срабатыванию одного из детекторов

8 5 23 10 30 21 14.

Остальные позиции строки заполняются случайным образом в заданном диапазоне значений, генерируются новые детекторы – вторичные детекторы, в которых содержится тоже самое сочетание, но размещается на разных позициях:

6 45 10 30 21 86 18
98 10 30 21 2 14 61
10 30 21 34 67 12 5.

Вторичные детекторы проверяются на соответствие с шаблоном «своего». При совпадении вторичные детекторы удаляются как лишние. Из оставшихся вторичных детекторов формируются шаблоны первичных детекторов. Число сгенерированных вторичных детекторов регулируется заданным числом вторичных детекторов, оставшихся после проверки, на соответствие с шаблоном «своего». Новые вторичные детекторы с позиции моделирования ИИС являются антителами, принадлежащих “чужому” (антигену).

Вторичные детекторы необходимы для проведения анализа входного сигнала и способствуют повышению эффективности распознавания «чужого», вызвавшего их появление. При повторном появлении «чужого» с похожими параметрами вторичные детекторы будут являться функцией памяти системы информационной безопасности на данный вид её нарушения.

Постоянный процесс создания вторичных детекторов для разных «чужих» будет приводить к неограниченному росту общего числа детекторов.

Предполагаемые нарушения безопасности информации и соответствующая реакция системы безопасности информации формируется как совокупность откликов всех детекторов (как первичных, так и вторичных).

Схема формирования набора детекторов показана на рисунке 2.

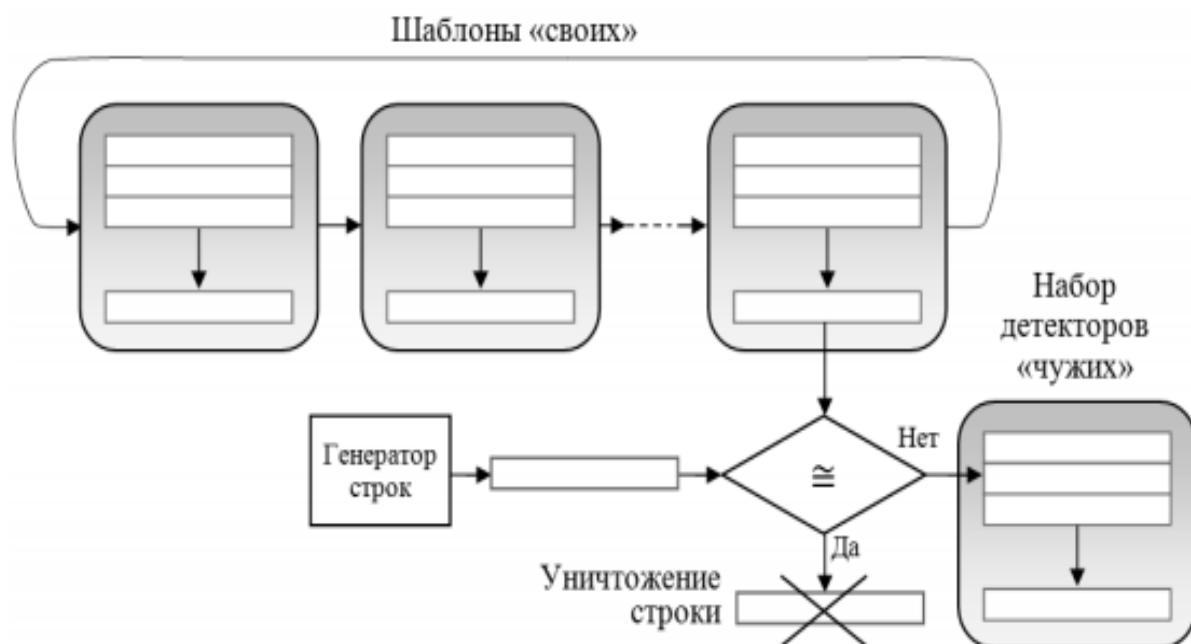


Рисунок 2 – Схема формирования набора детекторов

Для постоянного контроля детекторов на заданном уровне необходим какой-либо механизм их регулирования. Если сравнить ИИС с нервной системой, то можно встроить механизм определения первичных детекторов, которые ни разу не активировались в процессе анализа входного сигнала, и уничтожать их в количестве, пропорциональном количеству включаемых вторичных детекторов. В такой механизме также должна быть функция забывания, которая будет выбирать кандидатов на удаление по значению периода времени, прошедшего после их последней активации [3].

Формирование детекторов происходит во время функционирования системы информационной безопасности. Обучение и режим функционирования взаимосвязаны между собой и регулируются внутренними взаимодействиями элементов, лишь опосредованно стимулируемыми внешней средой. Система информационной безопасности, созданная по описанной схеме, будет представлять собой адаптивную самоорганизующуюся структуру, ориентированную на поддержание эффективного уровня обнаружения нарушений информационной безопасности в условиях произвольно изменяющихся внутренних состояний информационной системы и внешних воздействий.

После анализа были сделаны следующие выводы:

- качество мониторинга информационными процессами методами ИИС зависит от количества детекторов;
- для обнаружения «чужих» необходимо достаточное количество строк.

1.3 Способы выявления нарушений информационной безопасности и определение мер реагирования на нарушения

Процесс обнаружения вредоносной активности включают в себя обнаружение нарушений и аномалий. Нарушения – это атаки, которые используют уже известные слабые места в системах ИТ, а аномалии – это деятельность, исходящая от внешних злоумышленников. Процесс выявления аномалий состоит в том, что происходит сравнение поведения системы с неким шаблоном, принятым за эталон состояния системы, при этом происходит формирование БД. Процесс выявления нарушений состоит в том, что деятельность пользователя сравнивается с шаблонами нарушителей [4].

Большинство систем выявления нарушений и аномалий основываются на модели Деннинга. Суть данной модели основывается на: поддержании набора профилей для пользователей, обновлении профилей пользователей, согласовании записей подсистемы аудита, оповещении обо всех выявленных аномалиях. Для выявления аномальной активности применяются статистические методы сравнения, при этом сравниваются команды пользователя с нормальным поведением. Работу пользователя в системе возможно представить в виде модели на основе правил [4].

На рисунке 3 приведена схема функционирования системы обнаружений аномалий, использующей принципы ИИС.



Рисунок 3 – Схема функционирования системы обнаружений аномалий, использующей принципы иммунитета

Основными алгоритмами, основанных на методе иммунологического подхода являются:

- алгоритм отрицательного отбора;
- алгоритм негативной селекции;
- иммунный ответ и др.

Именно эти алгоритмы являются основой для моделей СЗИ, однако, необходимо их дополнение и модификация под конкретный вид функционирования.

В системах выявления атак используется следующий вариант применения иммунологического подхода: экспертные системы дополняются искусственной иммунологической системой для того, чтобы снизить частоту ложных срабатываний. Если в период обучения ИИС стала выявлять новые неизвестные атаки, то необходимо обновить и экспертную систему, если этого не сделать, то появляющиеся новые атаки не будут обнаруживаться экспертной системой.

Если же ИИС представлена самостоятельно функционирующей системой обнаружения атак, то при обработке трафика происходит обработка информации с целью выявления в нём злоупотреблений. При выявлении активности, принятой за атаку, происходит активация режима реагирования и ожидается вмешательство администратора безопасности. По сравнению с предыдущим методом, данный подход более быстрый.

Свойство адаптивности иммунологических систем позволяет решать отдельно взятые задачи идентификации угроз, сопоставления поведения пользователей с имеющимися в системе шаблонами, автоматически формировать новые правила при изменении поля угроз, а также реализовать систему защиты информации технической системы в целом.

Для выявления нарушений в ИИС также используется алгоритм отрицательного отбора.

В общем виде алгоритм отрицательного отбора формулируется следующим образом:

а) определяется понятие «свой», как нормальная динамика поведения системы, которая описывается совокупностью строк символов фиксированной длины. При этом значения данных в строках квантуются по уровням;

б) создается набор детекторов «чужих», каждый из которых не должен совпадать с шаблоном «своего». При этом используется правило частичного соответствия, согласно которому две строки совпадают тогда и только тогда, когда они идентичны в определенном числе смежных позиций;

в) при мониторинге новых поступлений данных сначала производится их квантование по уровням в формате, после осуществляется проверка изменений с помощью постоянного сопоставления с детекторами.

Срабатывание какого-либо детектора означает, что появилась измененная строка.

Описанный алгоритм отрицательного отбора опирается на три важных принципа:

- каждый вариант алгоритма уникален;
- процесс выявления изменений имеет вероятностный характер;
- надежная система должна обнаруживать не только заранее известные варианты изменений, но и любую чужеродную активность.

Алгоритм отрицательного отбора основывается на проверке совпадений.

На рисунке 4 представлен процесс генерации детекторов в алгоритме отрицательного отбора.

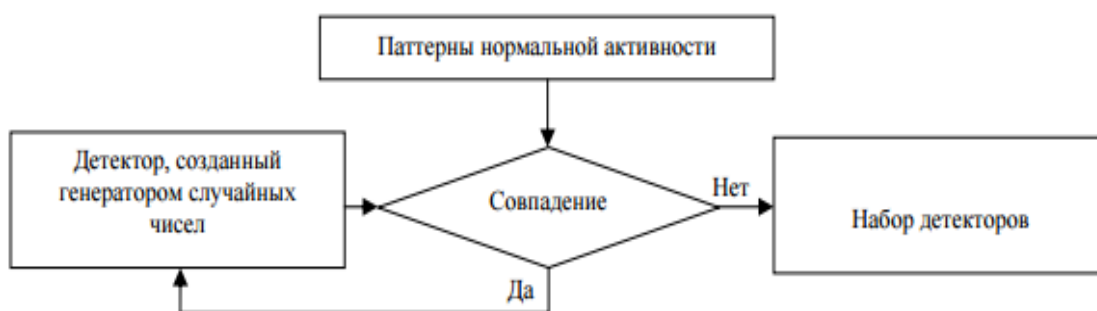


Рисунок 4 – Процесс генерации детекторов в алгоритме отрицательного отбора

Алгоритм отрицательного отбора, используемый в системах безопасности, в сильно упрощенной форме отражает лишь одну первоначальную стадию формирования иммунного ответа.

Первый пункт АОО моделирует принцип сетевого представления исходных данных системы информационной безопасности в виде совокупности клеток, подлежащих анализу на предмет чужеродности. Во втором пункте АОО показан принцип формирования детекторов, моделирующий создание в организме иммунокомпетентных клеток. В третьем пункте АОО путем проверки входного сигнала с детекторами моделируется процесс обнаружения чужеродных данных (антигенов). В рабочем режиме (режиме мониторинга) система функционирует в реальном масштабе времени и реализует третий пункт АОО.

Виды мер на нарушения информационной безопасности могут быть существенно различными: удаление зловредного программного кода,

заккрытие портов, проверка прав пользователей для определенных действий, ограничение действий пользователей и др. Принятие решения может осуществляться на разных уровнях иерархии: на уровне системы безопасности (например, встроенная антивирусная защита), на уровне всей защищенной системы (например, запросы на подтверждение полномочий для выполнения определенных действий), а также на более высоких уровнях иерархии управления (например, выдача сообщений администратору, принимающему окончательные решения). По этой причине при моделировании системы безопасности на принципах иммунологической системы политику безопасности защищенной системы условно ограничиваются простыми реакциями, сводящимися к выдаче сигналов о наличии нарушений информационной безопасности. Задача информационной целостности данных решается средствами самой системы (дублирование информации, уничтожение данных и т.п.).

1.4 Состояние и тенденции развития иммунологического подхода в информационной безопасности

В настоящее время иммунная система живого организма играет роль источника новых знаний об эффективных алгоритмах и структурах данных для использования в системах информационной безопасности.

За последнее десятилетие появилось большое количество моделей, использующих иммунологические системы в своей основе либо в качестве ключевых узлов. Иммунологические системы успешно применяются для решения задач оптимизации и классификации, а также искусственные иммунологические системы применяются для сжатия информации, кластеризации, поиска аномалий, машинного обучения, обработки неструктурированных данных и извлечения информации, компьютерной безопасности и адаптивного контроля.

Направления исследований иммунологических систем в данный момент можно формализовать как активную стадию применений и

исследований взаимосвязи природных и информационных систем из-за их схожести.

Сфера применения методов, основанных на принципах иммунологии весьма велика, такие методы имеют различные названия: искусственные иммунологические системы, иммунологические вычисления, системы, основанные на принципах иммунитета и др.

На рисунке 5 представлены основные направления исследований искусственных иммунологических систем.



Рисунок 5 – Направления исследований ИИС

В данный момент исследования иммунологических систем касаются использования достижений биологии в задачах компьютерных наук, совершенствования методов работы искусственных иммунных клеток, изучения функций аффинности и т.п.

Вычислительными способностями иммунологических систем занимается направление, названное иммунокомпьютингом.

Имунокомпьютинг позволяет с большой эффективностью решать следующие задачи:

- обучения с экспертом,
- самообучения (обучения без эксперта),
- группировки и классификации,
- представления результатов вычислений в пространстве образов.

Структурная схема иммунокомпьютинга для решения вышеперечисленных задач показана на рисунке 6.

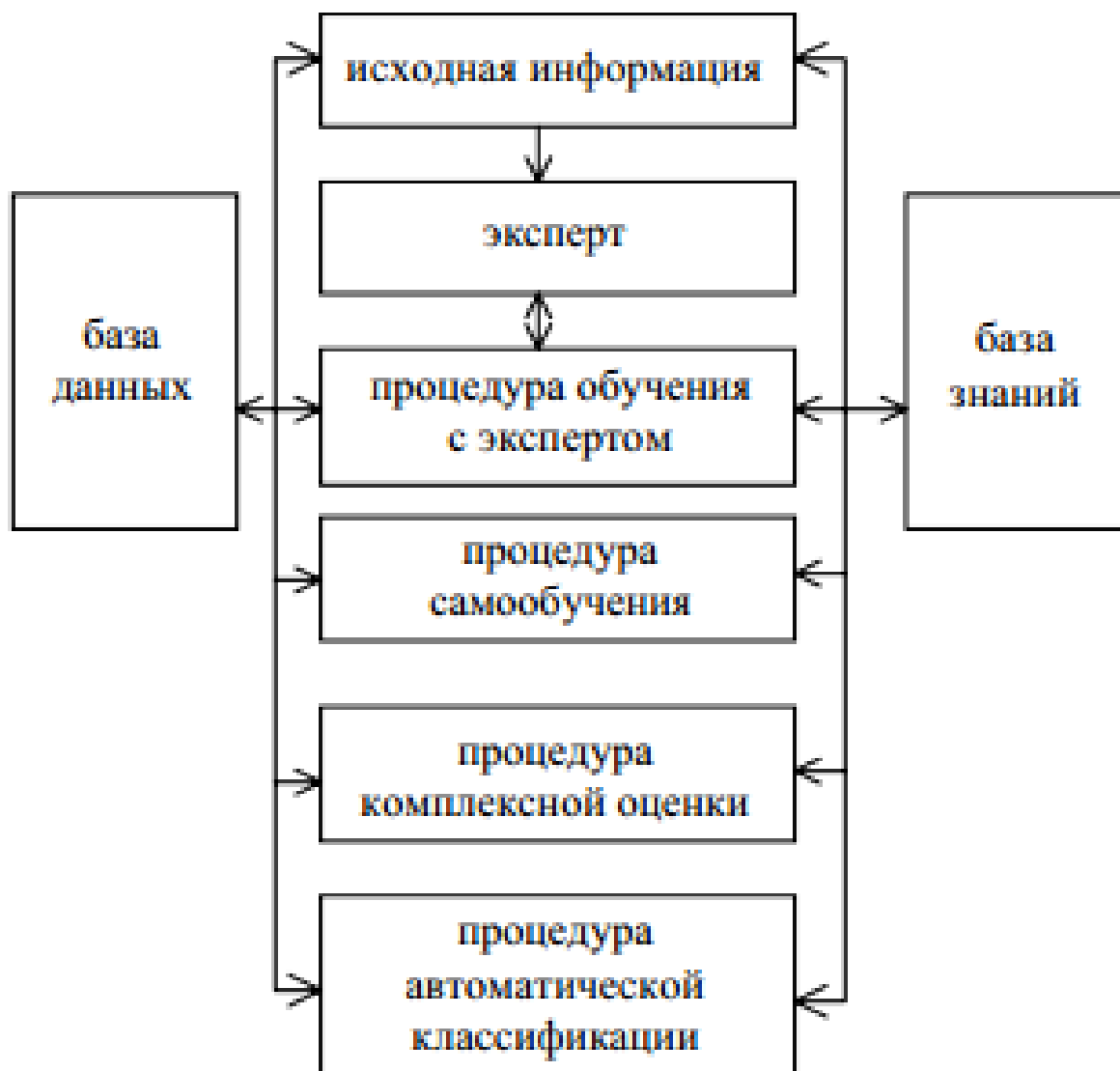


Рисунок 6 – Структурная схема иммунокомпьютинга

На основе исходной информации формируется база данных и база знаний. В базе данных содержатся данные о системе, в базе знаний хранится информация, отражающие закономерности и позволяющие получать новые

знания и прогнозировать в будущем возможные состояния, сведения о структуре и содержании БД. В базе знаний содержатся общедоступные данные и знания эксперта и др.

Одним из самых распространенных направлений ИИС является защита информации, где естественная иммунная система рассматривается как источник идей и методов решения задач информационной безопасности. Можно выделить два общих поднаправления исследований ИИС для информационной безопасности:

- иммунологические системы обнаружения вторжений, на базе АОО;
- иммунологические системы распознавания новых компьютерных вирусов.

Рассматриваются вопросы создания методов определения аномальной активности в ИИС в сравнении с её нормальным состоянием, обучения системы, анализа эффективности таких систем для защиты от определённого типа атак, а также ряд других научных и практических обобщений, составляющих теоретическую и методологическую базу настоящего исследования.

К перспективным моделям, использующим аналогию иммунной системы человека и ИТ, относятся следующие:

- модель оценки эффективности СЗИ ИТ;
- модель диагностики СЗИ ИТ;
- модель выявления предпосылок действия угроз (модель «мертвого кода»);
- корпоративная модель СЗИ;
- модель прогнозирования действия угроз и др.

При использовании метода иммунологического подхода в технологиях и организации СЗИ уменьшаются расходы и увеличивается эффективность.

До сих пор остались не решенными вопросы применения иммунологического подхода для автоматизации и интеллектуализации процессов информационной безопасности, так как открытым остается вопрос самостоятельного принятия решения во время обнаружения вторжения или аномалии.

В будущем, необходимо дальнейшее изучение и развитие данного направления в виду усложнения современных ИТ, необходимо, чтобы ИИС соответствовали динамике изменений.

1.5 Основные области применения иммунологического подхода

1.5.1 Применение иммунологического подхода

В настоящее время принципы работы и механизмы иммунологической системы заложены в основу для построения алгоритмов анализа данных, оптимизации и распознавания, систем информационной безопасности.

Сфера применения ИИС весьма велика, т. к. ИИС имеют многообразный характер.

Искусственные иммунологические системы легли в основу следующих средств информационной безопасности:

- средство сетевой самозащиты;
- средство антивирусной защиты;
- средство аутентификации;
- средство клавиатурного мониторинга;
- средство активного аудита и др.

Основные области применения иммунологического подхода в информационной безопасности представлены на рисунке 7.

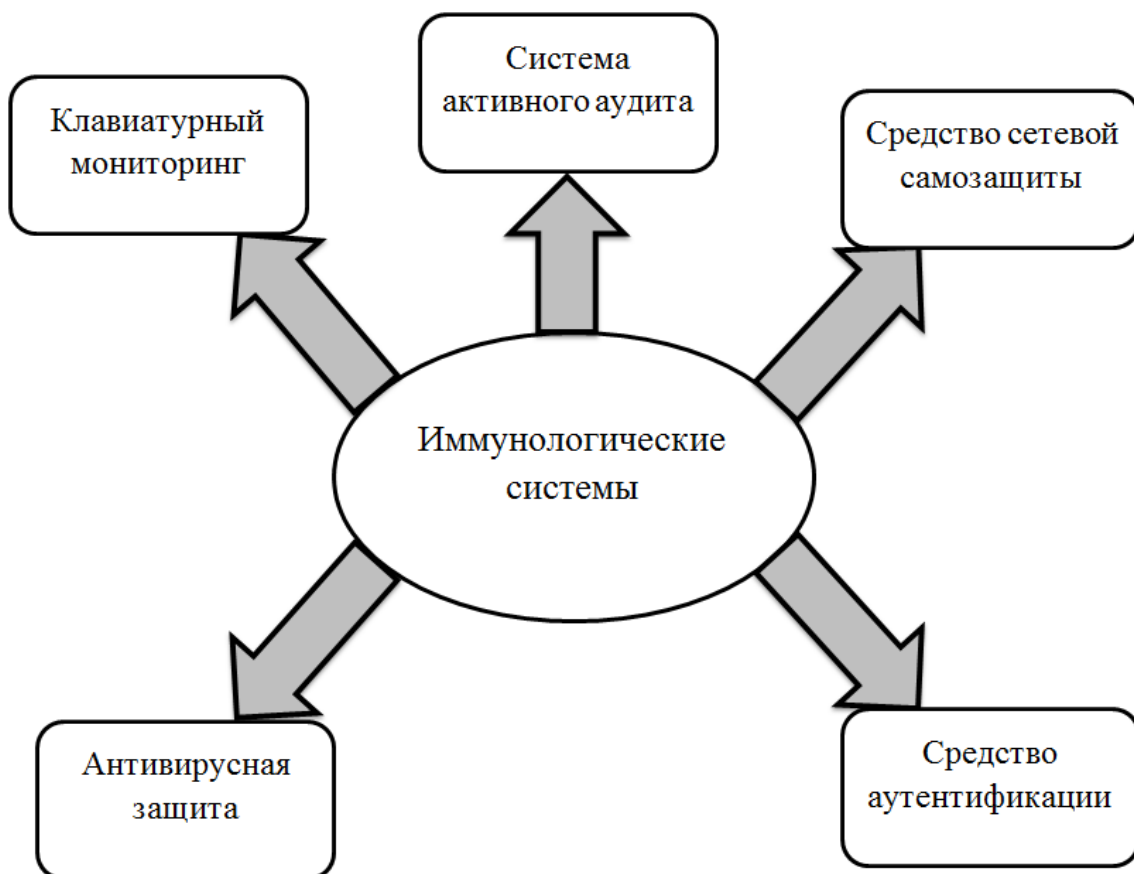


Рисунок 7 – Основные области применения иммунологического подхода

1.5.2 Средство сетевой самозащиты

Стоит отметить основные свойства иммунной системы человека:

- распределенная;
- самоорганизующаяся;
- легковесная.

Данными свойствами также должна обладать система обнаружения вторжений в сеть.

Система обнаружения вторжений, построенная на основе ИИС, подразделяется на основную и набор вторичных. В основной системе на базе ИИС происходят два процесса:

- эволюция геной библиотеки;
- негативная селекция данных.

На этапе эволюции генной библиотеки осуществляется сбор информации об аномалиях сетевого трафика. В генную библиотеку ИИС заносятся данные о кол-ве пакетов, их структуре, размере и др. Эта информация является формирующей для наборов детекторов. Учитывая сетевые протоколы формируются первичные данные для создания генной библиотеки. Если какой-либо детектор обнаружил вредоносную активность, то вносятся обновления в генную библиотеку, заносятся соответствующие данной активности новые гены. В генную библиотеку сохраняются только наиболее часто встречающиеся гены, а уже повторяющиеся гены удаляются. Затем генерируются наборы преддетекторов следующим образом: происходит комбинирование генов, затем с помощью механизма негативной селекции определяется их совместимость и несовместимость с нормальным сетевым трафиком. Происходит анализ информации о характере сетевого трафика, поток входных данных, поступающих от маршрутизатора. Суть заключается в создании ограниченного набора детекторов, с помощью которого можно было бы наиболее эффективно выявить сетевые аномалии. Такой тестовый набор детекторов рассылается по всем узлам сети, образуя вторичную систему обнаружения вторжений.

Известные сегодня алгоритмы негативной селекции основываются на вероятностных характеристиках, т. е. использует неполное совпадение. Изменение допустимого отклонения от эталона приводит к уменьшению или увеличению ложных срабатываний детекторов, чем меньше допустимое отклонение, тем чаще будет происходить обнаружение аномалии и наоборот. При выявлении вредоносной активности соответствующий ей детектор размножается и рассылается на остальные узлы системы. Решение о том, является ли активность действительно вредоносной принимается, если получены сигналы от нескольких узлов, а не от одного. В каждый узел и в основной системе обнаружения вторжений имеется коммуникатор, который осуществляет управление уровнем риска. Если какой-либо узел прислал сигнал об обнаружении вредоносной активности, то коммуникатор

увеличивает свой уровень риска и посылает сообщения другим коммутаторам, которые в свою очередь также увеличивают свои уровни риска. Если сразу несколько узлов обнаружили вредоносную активность за короткий промежуток времени, то уровень риска резко возрастает, и, если будет превышено пороговое значение риска, то администратору сети придёт уведомление об обнаружении вредоносной активности [5].

Структура системы обнаружения вторжений представлена на рисунке 8.

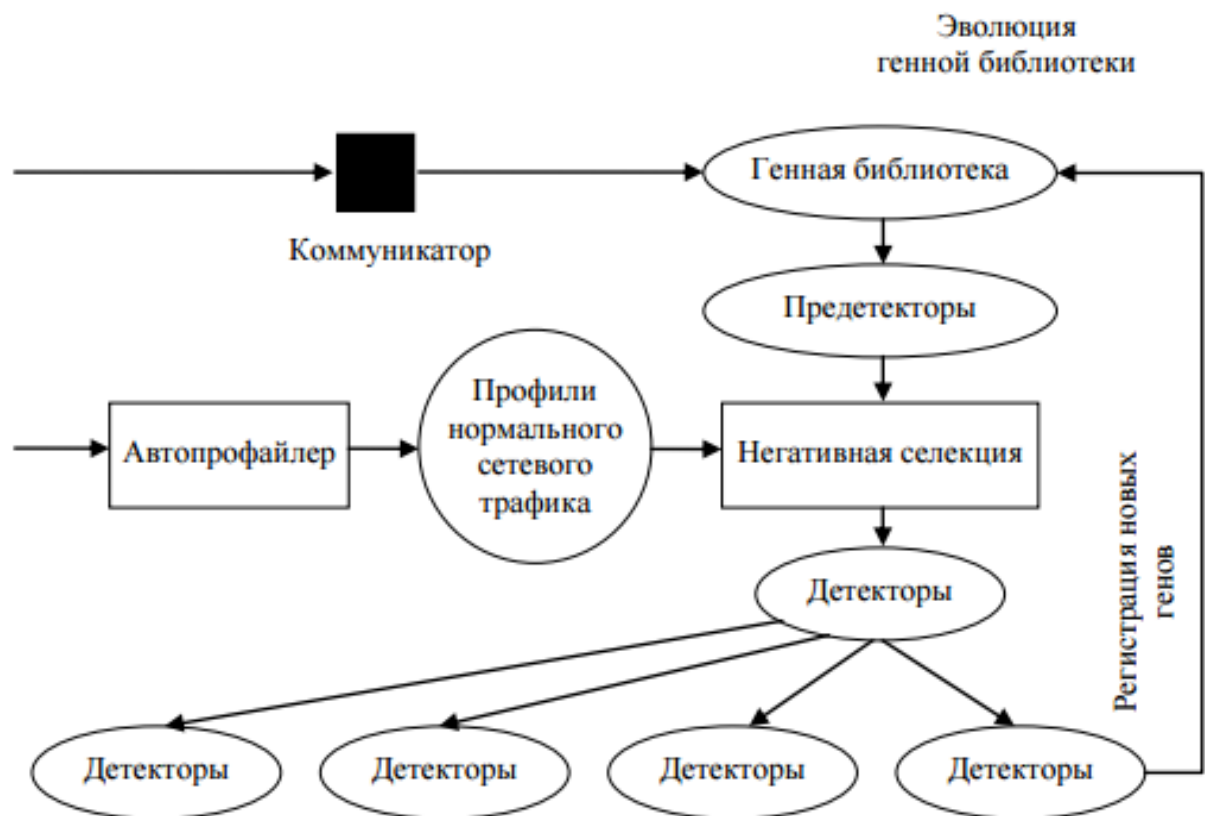


Рисунок 8 – Структура системы обнаружения вторжений

На рисунке 9 представлена классификация систем обнаружения вторжений с точки зрения иммунологического подхода.

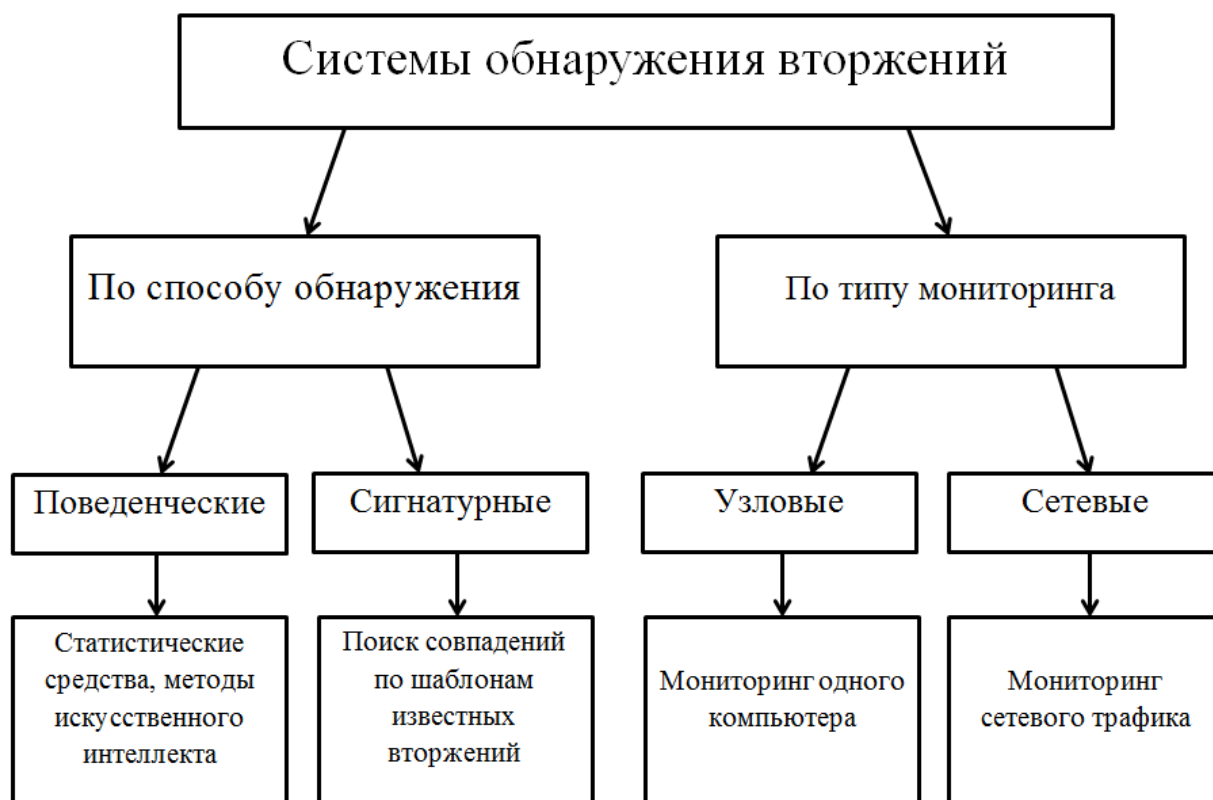


Рисунок 9 – Классификация систем обнаружения вторжений

Архитектура средства обнаружения вторжений состоит из:

- сенсорной подсистемы, которая осуществляет сбор событий;
- хранилища, в котором накапливаются первичные события и результаты анализа;
- подсистемы анализа, которая обнаруживает атаки и аномальную активность на основе данных, полученных от сенсоров;
- консоли управления, с помощью которой можно наблюдать за состоянием защищаемой системы, просматривать обнаруженные инциденты, осуществлять управление защищаемой системой.

1.5.3 Средство антивирусной защиты

Иммунная система человека весьма схожа с системой антивирусной защиты, т.к. их принципы работы очень похожи, выполняют они одни и те же функции. Для обнаружения заражения защищаемых данных и программных файлов весьма эффективным является использование такого подхода ИИС, как алгоритм отрицательного отбора.

В таблице 1 приведен сравнительный анализ иммунной системы человека и антивирусной программы.

Таблица 1 – Сравнительный анализ иммунной системы человека и антивирусной программы

Иммунная система	Антивирусная компьютерная программа
1. Назначение	
Иммунная система человека предназначена для защиты организма как от внутренних нарушений, так и от внешних вирусов.	Антивирусная компьютерная программа предназначена для обнаружения и удаления вредоносного кода, как от внешних угроз так и от заражения установленными программами.
2. Функционирование в случае обнаружения уже известных внешних угроз	
В случае попадания в организм человека уже известного вируса, иммунная система обнаруживает его и уничтожает.	В случае попадания в компьютер уже известного вируса антивирусная компьютерная программа обнаруживает его, изолирует и уничтожает.

Продолжение таблицы 1

Иммунная система	Антивирусная компьютерная программа
3. Функционирование в отношении неизвестных внешних угроз	
Иммунной системой человека неизвестный ранее вирус не обнаруживается и попадает в ткани организма, нанося вред организму.	В случае, если вирус неизвестен антивирусной компьютерной программе, она пропустит его, а он в свою очередь нанесет вред компьютеру.
4. Функционирование в случае обнаружения известных внутренних угроз	
При обнаружении известных внутренних заражений иммунитет должен их обнаруживать и уничтожать.	При обнаружении опасной активности уже установленного или устанавливаемого на компьютер ПО антивирус должен ограничить действие таких программ.
5. Функционирование в отношении неизвестных внутренних угроз	
В случае появления неизвестных внутренних угроз увеличивается риск образования заболеваний.	В случае появления неизвестных внутренних угроз увеличивается риск повреждения ОС и снижения работоспособности компьютера.

Продолжение таблицы 1

Иммунная система	Антивирусная компьютерная программа
6. Информация и обучение	
<p>Иммунная система человека получает базовую информацию и обучение при его рождении: объёмную базу данных от предыдущих поколений о всех известных до сих пор угрозах, а также способность выявлять новые угрозы. В процессе жизни организм сталкивается с новыми угрозами и иммунная система, получившая базовый иммунитет должна их выявлять и бороться с ними, после чего информация об угрозе сохраняется для дальнейшего быстрого реагирования (вторичный иммунитет). Иммунная информация записывается на мельчайших белковых молекулах - трансфер факторах.</p>	<p>Антивирусная компьютерная программа обладает БД о всех уже известных вирусах, а также способностью выявлять новые угрозы. Постоянно антивирусная система обновляется, т. е. получает информацию о новых вирусах и прочих угрозах и точно знает как выглядит потенциальный вредитель, благодаря чему надёжно защищает от них компьютер.</p>

Около 70 % вирусных атак осуществляется из внешней среды через точку входа в защищаемую сеть, и только около 30 % вирусных атак

являются внутренними. Необходимость в выявлении внешних угроз превышает, чем необходимость выявления внутренних угроз.

Использование ИИС заключается в том, что в случае обнаружения в сети признаков заражения происходит отправка образа нового вируса в антивирусный центр, через некоторое время создаётся обновление для антивирусной базы, которое рассылается по корпоративной сети с надобностью опередить распространение вируса. Данный метод противоречит иммунологическому подходу тем, что антивирусный центр находится вне самой системы, а в ИИС все процессы происходят внутри системы, данное отличие является весьма уязвимым местом в системе. Когда антивирусный центр находится за пределами защищаемой системы ИТ, нарушители могут сформировать канал для загрузки вирусов и вредоносных программ под видом обновления антивирусной базы, получить доступ к конфиденциальной информации в случае автоматической отправки на анализ подозреваемых на наличие вируса файлов.

Алгоритм отрицательного отбора легко находит изменения в зараженных файлах, однако, он предназначен для защиты постоянных файлов данных или программных файлов, а пользователи регулярно обновляют программное обеспечение, редактируют файлы данных. Это говорит о том, что эталон должен тоже постоянно меняться, соответствовать динамике изменений внутренней и внешней среды.

Для обнаружения компьютерных вирусов можно также использовать метод, основанный на принципе иммунного ответа. Суть данного метода состоит в следующем: известные вирусы выявляются по сигнатурам, а неизвестные вирусы выявляются по аномальной активности в системе.

Структура технологии антивирусной защиты на основе аналогии с иммунной системой человека представлена на рисунке 10.

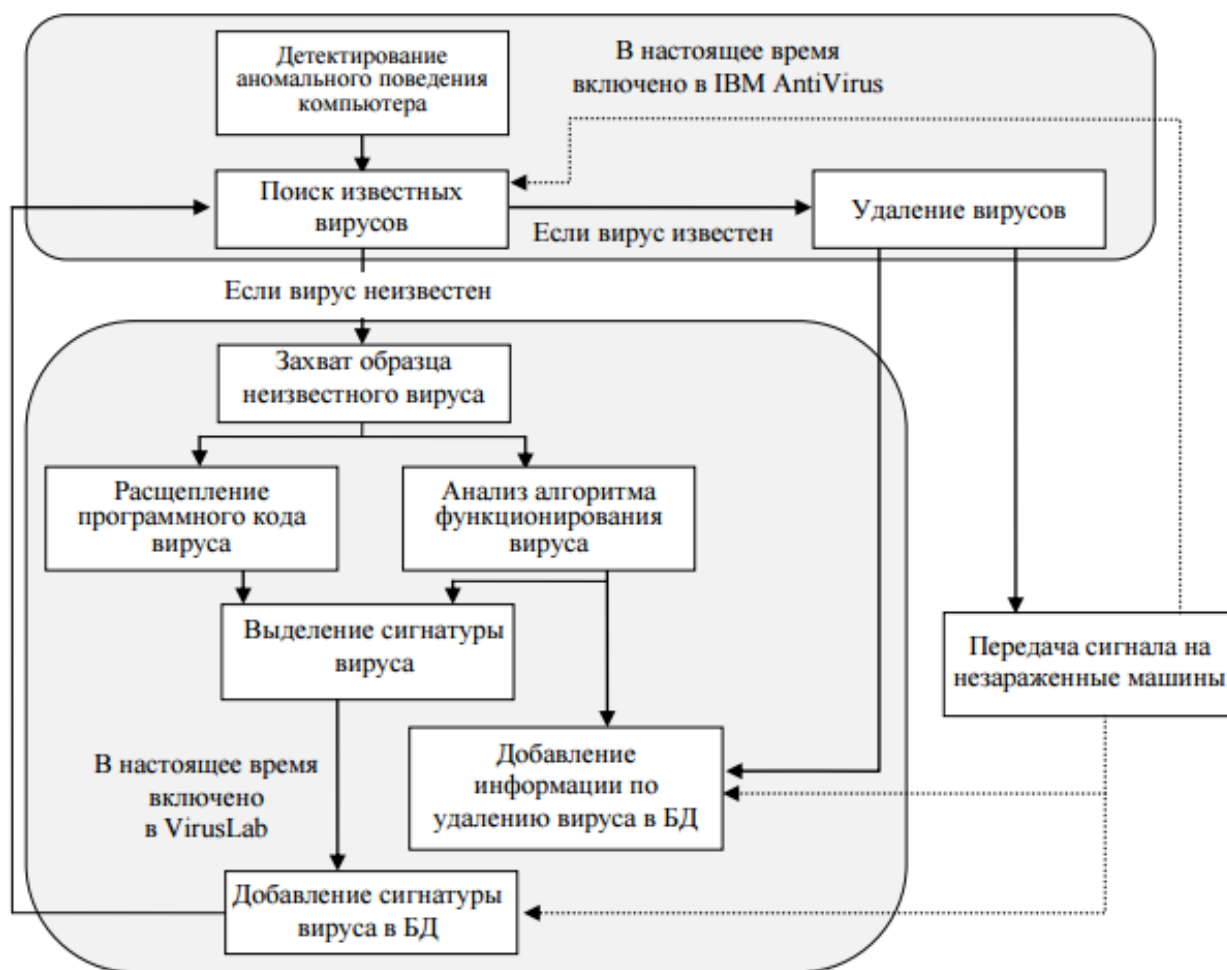


Рисунок 10 – Структура антивирусной защиты на базе иммунологических принципов

1.5.4 Средство аутентификации

Самым эффективным СЗИ при НСД является система аутентификации. Самой распространенной среди систем аутентификации является двухпоточная модель аутентификации, в которой используется множество обновляемых детектирующих наборов на основе иммунологического подхода. От иммунологической системы она наследует механизмы, которые дают возможность эффективно распознавать действия нарушителя. Первый поток аутентификации осуществляет в базе поиск уже встречавшихся угроз, а второй поток находит новые. Также от иммунологической системы наследуется механизм подтверждения результатов, который основан на получении сигнала от соседних детектирующих наборов при анализе массива данных, предоставляемых одним и тем же субъектом [5].

Структура двухпоточковой модели аутентификации представлена на рисунке 11.

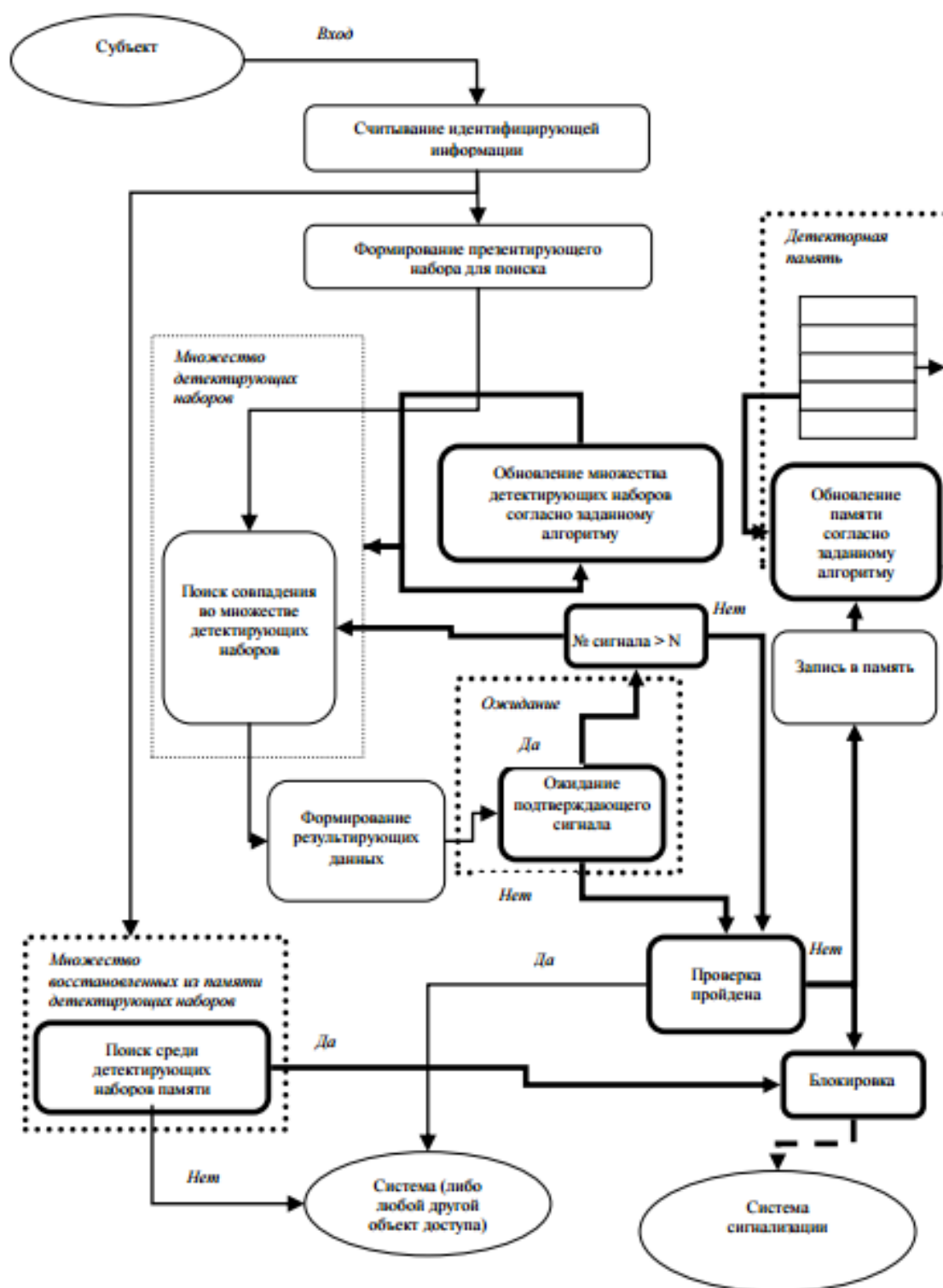


Рисунок 11 – Структура аутентификации с использованием обновляемого множества наборов

1.5.5 Средство клавиатурного мониторинга

Клавиатурный мониторинг является средством компьютерной безопасности, с его помощью осуществляется постоянная скрытая аутентификация пользователей. Для совершенствования средств КМ необходимо анализировать все действия пользователя целиком, а не по отдельности. Такой подход соответствует принципу работы ИИС. Иммунологический подход, используемый в КМ, основывается на АОО. Средство КМ работает следующим образом: во время обучения создается шаблон каждого пользователя, на основе которого формируются детекторы для обнаружения нарушений на определенном множестве возможных сочетаний клавиатурных параметров. Средство КМ обнаруживает нарушения по частоте срабатывания сформированных ранее детекторов [1].

С помощью КМ осуществляется постоянный анализ клавиатурного почерка пользователей компьютерных систем. КМ может функционировать в тайне от пользователей, в таком случае он является скрытым. На основе скрытого КМ решаются следующие задачи:

- ведение постоянной аутентификации пользователей;
- проведение оценки достоверности сообщений;
- выявление психофизических отклонений пользователей от нормального состояния;
- выявление пользователей компьютерных систем, которые совершили нарушения или злоупотребления полномочий.

Первая задача решается для того, чтобы создать базу данных для подразделения на "своих" и "чужих". Классификация пользователей на "своих" и "чужих" в биометрических системах решается двумя способами:

- с помощью верификации;
- с помощью идентификации.

При верификации в системе создаётся единственный эталон для каждого пользователя, информация о неизвестном пользователе сравнивается

только единственным эталоном. При идентификации же информация о неизвестном пользователе сравнивается со всеми эталонами пользователей. На эффективность работы систем КМ влияет точность и скорость осуществления верификации, которые зависят от способов представления и подразделения клавиатурных параметров. Клавиатурные параметры приводятся к некому структурированному виду, позволяющему выявить характерные признаки компьютерного почерка пользователя, отличающегося от других. Во время обучения системы КМ с помощью характерных признаков и строятся шаблоны «своих», иными словами, эталон поведения пользователя. Во время работы осуществляется сравнение характеристик компьютерного почерка работающего пользователя с уже сложившимся клавиатурным эталоном пользователя. Затем, если же были обнаружены отклонения, работа пользователя блокируется системой КМ.

Данный метод соответствует иммунологическому принципу выявления аномалий в ИС. В ИИС входная информация анализируется для выявления аномалий путем сравнения с детекторами. Сравнение производится не в одиночных, а сразу в нескольких смежных позициях. Ширина зоны сравнения задается параметром r , который определяет степень связности событий и называется в иммунологии степенью аффинности.

Как уже упоминалось выше, работа КМ основывается на АОО, принципиальным отличием АОО от обычного распознавания, является тот факт, что эталон формируется и используется лишь при обучении ИИС для создания детекторов. Во время распознавания неизвестные образы сравниваются не с эталонами, а с детекторами.

Применение иммунологического подхода в КМ даёт возможность получить системы, со следующими свойствами:

а) при работе в системе КМ нескольких пользователей, происходит увеличение числа эталонов, а при использовании АОО, наоборот, кол-во детекторов остается постоянным;

б) АОО проявляет большую устойчивость к шумам из-за высоко распределенной массовой обработки данных;

в) в АОО обнаружение «чужих» производится в темпе поступления входных данных и отображается частотой активации детекторов.

Таким образом, применение иммунологического подхода для создания средства КМ является весьма актуальным.

1.5.6 Система активного аудита

Аудит системы становится всё более применяемым в области обеспечения ИБ.

Система активного аудита – это процесс получения качественных и количественных показателей о состоянии системы в сравнении с эталонными показателями и критериями безопасности [6].

Суть аудита заключается в проверке системы и сравнении полученных результатов с эталоном. Выделяются основные составляющие аудита, которые в свою очередь могут различаться для разных видов аудита:

- средства и способы проверки системы;
- результат проверки системы;
- эталон для сравнения результатов проверки системы.

Самым распространенным является активный аудит – исследование состояния защищенности системы с точки зрения нарушителя, который является хорошим специалистом в области информационных технологий и обладает навыками реализации угроз.

Алгоритм действий активного аудита сводится к тому, что с помощью специального программного обеспечения и методов осуществляется сбор информации о состоянии системы сетевой защиты.

На рисунке 12 представлена структура системы активного аудита.

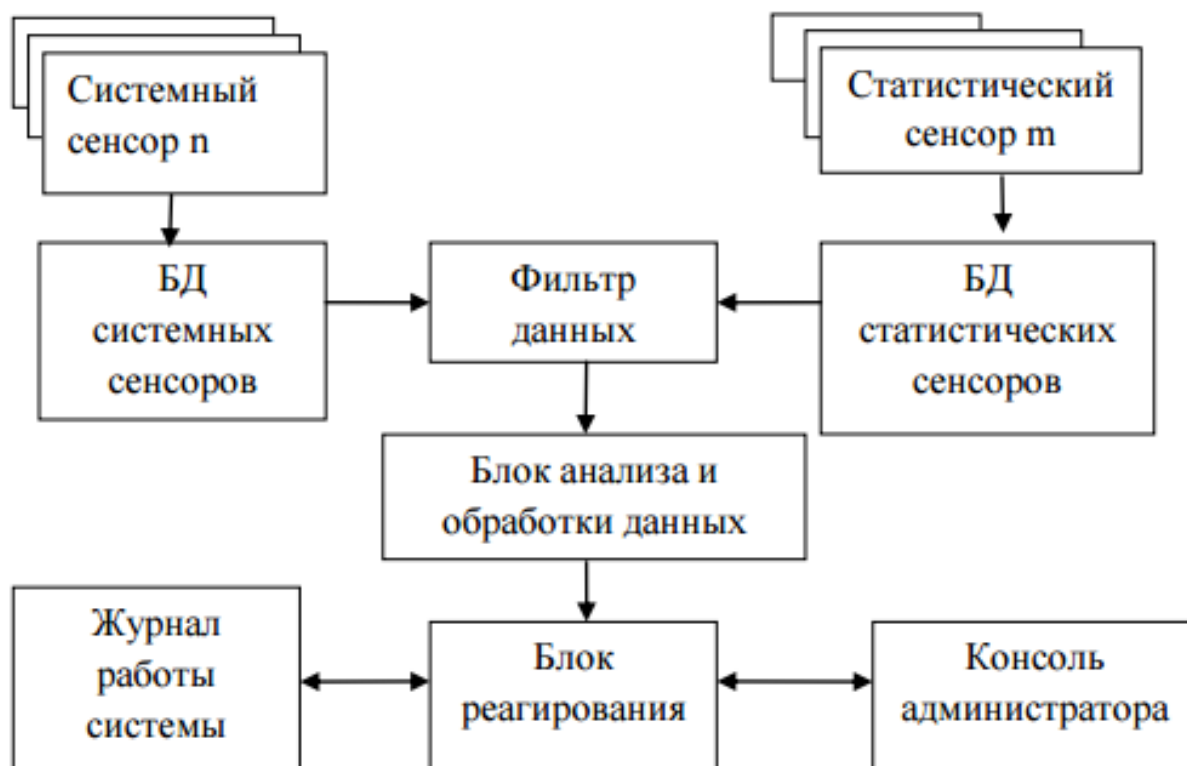


Рисунок 12 – Структура системы активного аудита

Система активного аудита состоит из:

- набора сенсоров для проверки информации о работе информационной системы и действиях пользователей;
- базы данных, где хранятся полученные результаты в виде отчётов;
- блока анализа и обработки данных, который проводит обработку входящих данных и осуществляет управление информационной системой;
- блока реагирования, который выполняет функцию ответа;
- сервера администратора;
- журнала учёта активного аудита.

Набор сенсоров предназначен для сравнения показателей системы и действий пользователей, осуществления оповещений для обработки в блоке анализа и обработки данных об уже известных событиях. Также осуществляется анализ и прогнозирование поведения всех пользователей системы. Для пользователя создаётся отдельный профиль, в который

записывается вся информация о его работе в системе с определенной периодичностью, которую задает администратор безопасности системы.

Для повышения эффективности работы системы в ней есть фильтр данных, который удаляет уже встречавшиеся инциденты. Также фильтр данных необходим для экономии памяти.

Для повышения эффективности анализа входящей информации необходимо:

- обеспечить надёжное хранение поступающей информации до её обработки системой активного аудита;
- обеспечить быструю обработку сигналов сенсоров с целью обнаружения атак системой активного аудита и принятия решения по предотвращению атаки;
- обеспечить безопасное хранение необходимой информации в целях сохранения истории атак и обновления профилей пользователей.

При обнаружении инцидента система активного аудита принимает решение об ответной реакции. Система принятия решения основывается на нечёткой логике, с помощью которой можно принять верное решение, которое зависит от типа объекта, подвергающегося угрозе и условий выполнения нарушения.

Ответная реакция может быть следующей:

- уведомление администратора системы об инциденте;
- блокирование пользователя в системе;
- перезагрузка рабочей станции;
- выгрузка программ из памяти рабочей станции и др.

При проектировании системы активного аудита следует учитывать, что вызовы процессов управления аппаратными средствами системы могут привести к более опасным повреждениям, нежели вызовы пользовательских процессов. Также имеется возможность отслеживать последствия двух

одновременных атак. Обнаруживать источники аномальной активности позволяют короткие последовательности вызовов самой системы.

2 Комплекс моделей иммунологических систем

2.1 Функциональная модель иммунологической системы

Функциональная модель необходима для упорядочивания взаимосвязей подцелей и функциональных операций.

Была разработана функциональная модель иммунологической системы, при этом были выделены следующие уровни функционирования:

- уровень управления;
- уровень сетевых узлов;
- прикладной уровень;
- уровень компонентов.

На уровне управления осуществляется управление системой защиты информации. Данный уровень имеет иерархическую структуру, которая состоит из нескольких центров управления, в свою очередь каждый центр управления является самостоятельным. Центр управления может состоять из нескольких серверов администрирования, а каждый сервер администрирования управляет определенной частью системы защиты информации. Управление комплексной системой защиты информации осуществляется на основании политики безопасности, которая задаёт правила функционирования для всех программных средств защиты информации.

Уровень сетевых узлов представляет собой категории программных средств защиты информации, направленных на защиту различных узлов сети (сервера, шлюзы, рабочие станции, мобильные устройства и др.). На данном уровне определяются типы и количество узлов сети, происходит их сегментация, а также определяются соответствующие типы программных средств защиты, определяется степень распределенности проектируемой комплексной системы защиты от нарушений информационной безопасности.

Прикладной уровень представляет собой комплекс программного обеспечения, направленного на защиту узлов сети в зависимости от их

назначения и используемой операционной системы. Данный уровень оказывает влияние на гетерогенность проектируемой комплексной системы защиты от нарушений информационной безопасности, определяет типы политик безопасности.

Уровень компонентов состоит из модулей, входящих в состав программного обеспечения и направленных на защиту от конкретных угроз [7].

Для создания функциональной модели ИИС необходимо для начала определить минимальный набор требований к системе, которым она должна удовлетворять.

Описанная выше схема позволяет создать шаблон системы защиты от нарушений информационной безопасности на основании сформированного списка функциональных операций, выполняемых системой защиты информации.

Шаблон системы защиты информации на базе иммунологического подхода состоит из:

- набора функциональных операций, выполняемых иммунными механизмами защиты;
- набора функциональных операций, выполняемых системой управления программными средствами защиты.

Для формирования шаблона системы защиты информации был составлен список функциональных операций, выполняемых иммунными механизмами защиты и системой управления этими механизмами. Затем был произведен анализ списка функциональных операций для выявления наиболее значимых и важных с точки зрения их применяемости в искусственных иммунологических системах и системах защиты информации экспертами по информационной безопасности.

В список функциональных операций были включены следующие функциональные операции:

- защита рабочих станций;
- защита файловых серверов;
- защита интернет шлюзов;
- защита серверов баз данных;
- защита всей системы;
- предупреждение потенциальных угроз;
- обнаружение угроз;
- выявление угроз;
- ликвидация угроз;
- ликвидация последствий угроз;
- оповещение о вредоносной активности;
- блокирование части функций системы;
- прекращение работы всей системы;
- формирование отчетных документов;
- ожидание принятия решения;
- идентификация лиц, претендующих на доступ;
- регистрация обращений к защищаемым ресурсам;
- проверка полномочий;
- реагирование при попытках несанкционированных действий пользователей;
- опознавание объекта или субъекта по предъявленному идентификатору.

Следует отметить, что в данном исследовании необходимо полагаться на компетентность экспертов, т.к. выявление критериев значимости функциональных операций трудно воссоздать на практике.

В качестве экспертов мною было выбрано 3 специалиста, обладающих достаточным опытом в области информационной безопасности, чья профессиональная деятельность непосредственно связана с обеспечением информационной безопасности в различных организациях:

- студентка кафедры ИБСТ Попова Марина Сергеевна;
- программист кафедры ИБСТ Тикин Михаил Сергеевич;
- инженер 1-ой категории АО «ПНИЭИ» Сулов Валентин Александрович.

Опрос экспертов по информационной безопасности осуществлялся методом анкетирования. В анкете необходимо было проранжировать функциональные операции с точки зрения их опыта и рассуждений, а также значимости. При этом самая значимая функциональная операция должна занять первое место, а наименее значимая – последнее место.

Основное назначение системы информационной безопасности – это обеспечение безопасности информации и функционирование при любых условиях.

Основные задачи, предъявляемые к ИИС:

- защита объектов системы;
- определение подцели обеспечения безопасности;
- мера реагирования на инцидент;
- управление доступом.

Проанализировав заполненные экспертами по информационной безопасности анкеты, были выявлены следующие основные функциональные операции:

- защита всей системы;
- предупреждение потенциальных угроз;
- оповещение о вредоносной активности;
- реагирование при попытке несанкционированных действий.

Заполненные экспертами по информационной безопасности анкеты представлены в Приложении А.

На основе анализа анкет, заполненных экспертами по информационной безопасности, был создан шаблон функциональной модели иммунологической системы, который представлен на рисунке 13.

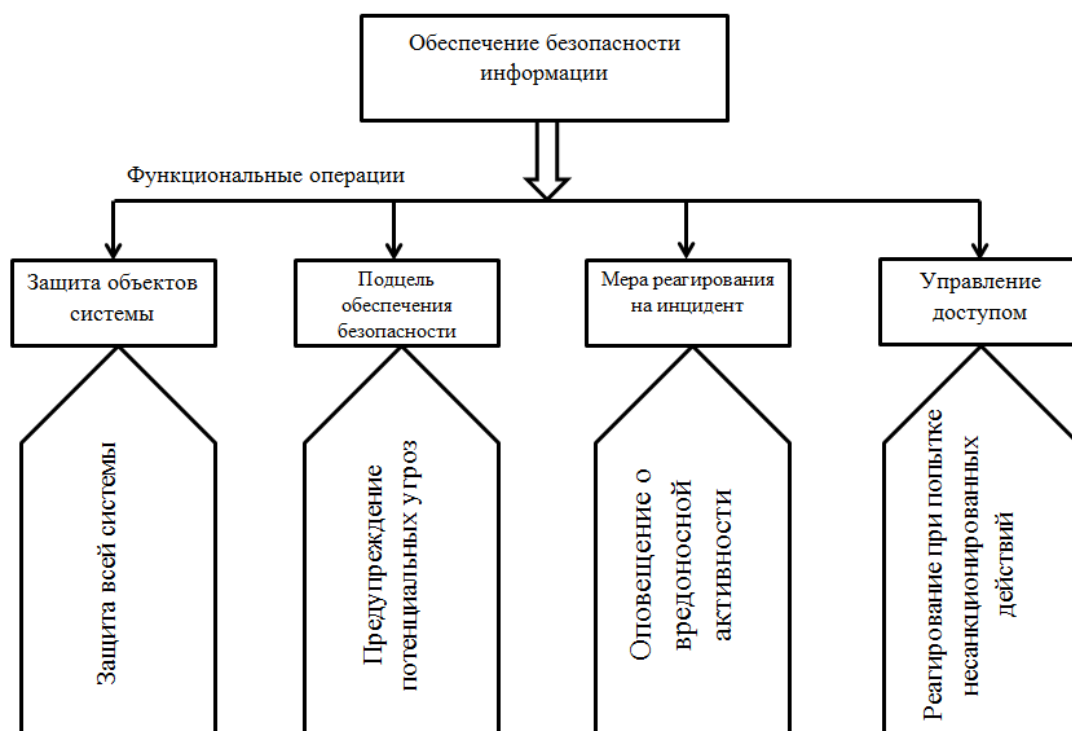


Рисунок 13 – Функциональная модель иммунологической системы защиты информации

В зависимости от типа деструктивного воздействия, его направленности и последствий для системы подбираются и формируются группы принятия решений определенного типа, которые являются наиболее эффективными именно для этой конкретной ситуации. Были выделены следующие общие принципы функционирования искусственных иммунологических систем:

- способность регистрировать, выявлять и определять место деструктивного воздействия на элемент структуры системы;
- проводить оценку серьезности дестабилизирующих воздействий на ранних стадиях их реализации;
- идентифицировать тип деструктивного воздействия на основе оперативного анализа и принимать решения в условиях не полной определенности имеющейся информации и при необходимости генерировать сигнала тревоги;

- вырабатывать защитные механизмы, специфичные к соответствующему деструктивному воздействию;
- запускать процесс восстановления (регенерации) поврежденных элементов.

2.2 Модель принципа действия иммунологической системы

На основе метода индукции (исследования, обобщения результатов) первой главы данной дипломной работы была создана модель принципа действия иммунологической системы.

Можно выделить следующие этапы функционирования иммунологических систем:

- а) детекторы идентифицируют любую аномальную активность;
- б) идентификаторы распознают аномальную активность как определенный тип нарушения, при условии нахождения в базе знаний соответствующей сигнатуры или выявление отклонения по отношению к эталону поведения;
- в) идентификаторы распознают аномальную активность как определенный тип нарушения, при условии нахождения в базе знаний соответствующей сигнатуры или выявление отклонения по отношению к эталону поведения;
- г) формируются тестовые наборы механизмов защиты согласно алгоритму, который генерируется базой знаний;
- д) проверка эффективности тестового набора механизмов защиты;
- е) принятие решения относительно выбора набора механизмов защиты;
- ж) выдача подсистемой обработки сигнала модулю реагирования относительно реагирования на нарушение с помощью набора механизмов защиты;
- и) самоорганизация и оценка подсистемой обратной связи и детекторами эффективности использования набора механизмов защиты,

пополнение базы знаний новой информацией, расследование и анализ нарушения, выработка сигнала относительно превентивных действий.

Адаптивное самообучающееся средство защиты информации, основанное на принципах иммунологических систем, начинает свою работу с генерации детекторов, чтобы соответствие детекторов и сведений о правильной работе не превышало задаваемого входного значения. Алгоритм генерации детекторов представлен на рисунке 14.

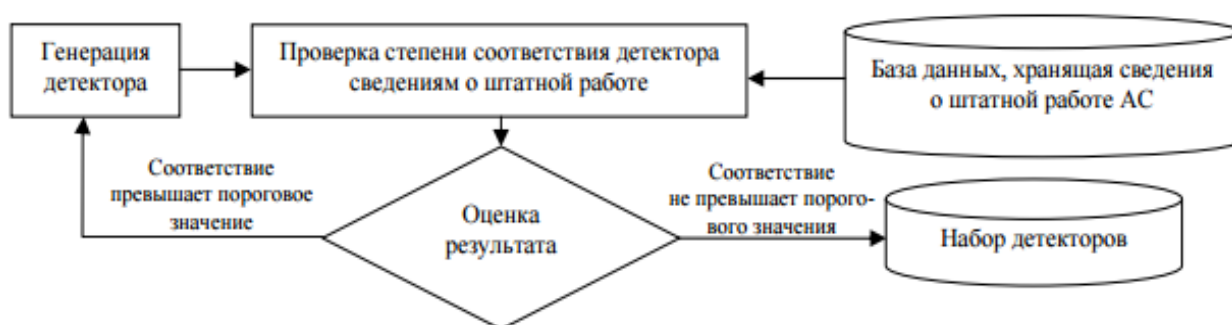


Рисунок 14 – Алгоритм процесса генерации детекторов

В режиме функционирования средство собирает данные об автоматизированной системе и проверяет их на соответствие сгенерированным ранее детекторам. Алгоритм функционирования адаптивного самообучающегося средства защиты информации представлен на рисунке 15.

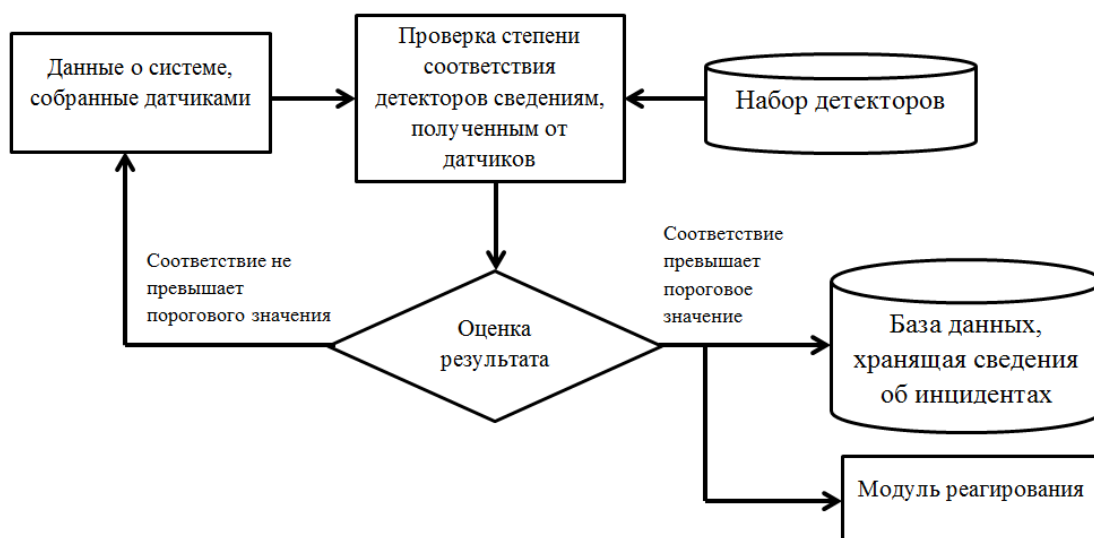


Рисунок 15 – Алгоритм функционирования средства защиты информации

Если один из детекторов соответствует полученным данным, эти данные заносятся в журнал учёта инцидентов информационной безопасности и передаются в модуль реагирования.

Модуль выявления угроз основывается на алгоритме отрицательного отбора или его модификациях.

Шаг 1. Определяется понятие «своё» как совокупность A строк длины P над конечным алфавитом, которую и необходимо защищать. Под совокупностью A и понимается информация, которая представляет собой программу, файл данных, программное обеспечение.

Шаг 2. Создается набор детекторов D , каждый из которых не должен соответствовать любой строке из A , две строки соответствуют друг другу, тогда и только тогда, когда они совпадают по крайней мере в r следующих друг за другом позициях, где r – целочисленный параметр.

Шаг 3. Происходит проверка A на наличие модификаций путем непрерывного сравнения детекторов D с элементами совокупности A . Если какой-либо детектор совпадет, это будет означать, что произошла модификация, т.к. детекторы отобраны таким образом, чтобы не соответствовать строкам из A .

Описанный выше АОО опирается на следующие принципы:

- каждый вариант алгоритма уникален;
- процесс выявления модификаций имеет вероятностный характер;
- надежная система защиты информации должна уметь обнаруживать не только уже известные варианты модификаций, но и любую аномальную активность.

2.3 Структурная модель иммунологической системы

Началом любой системы является её структура, которая даёт возможность распознать взаимосвязи между элементами системы и подсистемами. Структурная модель строится только после создания функциональной модели и модели принципа действия, т. к. сначала

необходимо проанализировать какие элементы системы будут выполнять выбранные функциональные операции.

Структура адаптивного самообучающегося средства защиты информации, созданного на основе принципов работы иммунологической системы должно иметь следующие элементы:

- датчики, которые собирают информацию о текущем состоянии системы;
- модуль выявления угроз, который при помощи аппарата искусственных иммунологических систем определяет, являются ли события, полученные от датчиков, инцидентами информационной безопасности;
- модуль хранения данных, который содержит сведения об инцидентах информационной безопасности, журнал учёта инцидентов, информацию о параметрах алгоритма функционирования;
- модуль реагирования, который осуществляет действие системы при обнаружении нарушения информационной безопасности.

Реагирование на нарушение определяется политикой безопасности и зависит от степени возможного ущерба. Это может быть оповещение об инциденте, блокирование части функций системы, прекращение работы системы и другие действия, а также их совокупность.

Структура иммунологической системы представлена на рисунке 16.



Рисунок 16 – Структура иммунологической системы

ЗАКЛЮЧЕНИЕ

В результате выполнения дипломной работы были исследованы: предпосылки и возможности создания моделей иммунных систем в информационной безопасности, регулирование взаимоотношений защищенной системы с внешней средой, способы выявления нарушений информационной безопасности и определение мер реагирования на нарушения, состояние и тенденции развития иммунологического подхода в информационной безопасности, основные области применения иммунологического подхода. Было рассмотрено применение принципов функционирования механизмов иммунологической системы в задаче построения средств защиты информации.

В результате практической части дипломной работы были созданы: функциональная модель иммунологической системы, модель принципа действия иммунологической системы, структурная модель иммунологической системы.

В процессе выполнения дипломной работы была написана научная статья [11].

Задание на дипломное проектирование выполнено в полном объеме.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Брюхомицкий Ю.А. Иммунологический подход к организации клавиатурного мониторинга/ Известия Южного федерального университета. Технические науки №2. – 2014. – 33-41с.
- 2 Брюхомицкий Ю.А. Использование принципов построения и функционирования иммунных систем в компьютерной безопасности/ Материалы XII Международной научно-практической конференции «Информационная безопасность»
- 3 Брюхомицкий Ю.А. Предпосылки создания моделей компьютерной безопасности на принципах функционирования иммунных систем/ Известия Южного федерального университета. Технические науки №1. – 2012. – 159-163 с.
- 4 Калач А.В., Немтина Е.С. Интеллектуальные средства и моделирование систем защиты информации/ Интернет-журнал «Технологии техносферной безопасности». – 2011. – 1-8 с.
- 5 Осовецкий Л.Г. Безопасность информационного общества и иммунология информационных технологий/ Программные продукты, системы и алгоритмы №1, – 2012. – 2-6 с.
- 6 Петренко С.А. Аудит безопасности Intranet. – М.: ДМК Пресс, 2002. – 386 с.
- 7 Романюха А.А. Искусственные иммунные системы и их применение / Под ред. Д. Дасгупты: Пер. с англ. – М.: Физматлит, 2006. – 344 с.
- 8 Строкань Д.А. Иммунные информационные системы: моделирование и анализ потребительского качества. – Ростов-на-Дону: Ростовский государственный экономический университет (РИНХ), 2012. – 11-12 с.
- 9 Bersini H., Varela F. The immune learning mechanisms: Recruitment reinforcement and their applications
- 10 De Castro Leandro N. Artificial Immune Systems: A new Computational Intelligence Approach. – Springer, 2002. – P.57 – 58

11 Никулина И.А. Иммунологические системы в обеспечении информационной безопасности // Молодежь. Наука. Инновации: Труды XIII Международной научно-практической интернет-конференции/ Под ред. И.В. Палаткина, Н.А Виноградовой - Пенза: Издательство ПКИТ ФГБОУ ВО «МГУТУ им. К.Г. Разумовского (ПКУ)», 2016. – С. 48-51

ПРИЛОЖЕНИЕ А

(обязательное)

Анкеты, заполненные экспертами по информационной безопасности

Ф.И.О. эксперта _____

Должность, научная степень _____

Необходимо, в каждом разделе расставить коэффициенты значимости от 1 до 5, при этом самой значимой функциональной операции должен быть присвоен коэффициент 1, а наименее значимой – коэффициент 5.

Перечень функциональных операций, выполняемых иммунными механизмами защиты и системой управления этими механизмами.

Функциональная операция	Коэффициент значимости (от 1 до 5)
Защита объектов системы	
защита рабочих станций	
защита файловых серверов	
защита интернет шлюзов	
защита серверов баз данных	
защита всей системы	
Подцели обеспечения безопасности информации	
предупреждение потенциальных угроз	
обнаружение угроз	
выявление угроз (возможности появления угроз)	
ликвидация угроз	
ликвидация последствий угроз	
Мера реагирования на инцидент	
оповещение о вредоносной активности	
блокирование части функций системы	
прекращение работы всей системы	
формирование отчетных документов	
ожидание принятия решения	
Управление доступом	
идентификация лиц, претендующих на доступ	
регистрация обращений к защищаемым ресурсам	
проверка полномочий	
реагирование при попытках несанкционированных действий	
опознавание объекта или субъекта по предъявленному идентификатору	

Дата заполнения и подпись _____

Ф.И.О. эксперта _____

Должность, научная степень _____

Необходимо, в каждом разделе расставить коэффициенты значимости от 1 до 5, при этом самой значимой функциональной операции должен быть присвоен коэффициент 1, а наименее значимой – коэффициент 5.

Перечень функциональных операций, выполняемых иммунными механизмами защиты и системой управления этими механизмами.

Функциональная операция	Коэффициент значимости (от 1 до 5)
Защита объектов системы	
защита рабочих станций	
защита файловых серверов	
защита интернет шлюзов	
защита серверов баз данных	
защита всей системы	
Подцели обеспечения безопасности информации	
предупреждение потенциальных угроз	
обнаружение угроз	
выявление угроз (возможности появления угроз)	
ликвидация угроз	
ликвидация последствий угроз	
Мера реагирования на инцидент	
оповещение о вредоносной активности	
блокирование части функций системы	
прекращение работы всей системы	
формирование отчетных документов	
ожидание принятия решения	
Управление доступом	
идентификация лиц, претендующих на доступ	
регистрация обращений к защищаемым ресурсам	
проверка полномочий	
реагирование при попытках несанкционированных действий	
опознавание объекта или субъекта по предъявленному идентификатору	

Дата заполнения и подпись _____

Ф.И.О. эксперта _____

Должность, научная степень _____

Необходимо, в каждом разделе расставить коэффициенты значимости от 1 до 5, при этом самой значимой функциональной операции должен быть присвоен коэффициент 1, а наименее значимой – коэффициент 5.

Перечень функциональных операций, выполняемых иммунными механизмами защиты и системой управления этими механизмами.

Функциональная операция	Коэффициент значимости (от 1 до 5)
Защита объектов системы	
защита рабочих станций	
защита файловых серверов	
защита интернет шлюзов	
защита серверов баз данных	
защита всей системы	
Подцели обеспечения безопасности информации	
предупреждение потенциальных угроз	
обнаружение угроз	
выявление угроз (возможности появления угроз)	
ликвидация угроз	
ликвидация последствий угроз	
Мера реагирования на инцидент	
оповещение о вредоносной активности	
блокирование части функций системы	
прекращение работы всей системы	
формирование отчетных документов	
ожидание принятия решения	
Управление доступом	
идентификация лиц, претендующих на доступ	
регистрация обращений к защищаемым ресурсам	
проверка полномочий	
реагирование при попытках несанкционированных действий	
опознавание объекта или субъекта по предъявленному идентификатору	

Дата заполнения и подпись _____

ПРИЛОЖЕНИЕ Б

(обязательное)

Проверка ВКР на оригинальность

Протокол

проверки на оригинальность в системе «Антиплагиат.ВУЗ» выпускной квалификационной работы на тему «Иммунологические системы в обеспечении информационной безопасности» студентки 6 курса Ирины Александровны Никулиной направления очной формы обучения направления подготовки 10.05.02, специальности «Информационная безопасность телекоммуникационных систем».

Руководитель ВКР В.А. Сулов

Информация о документе:

Имя исходного файла: ВКР_Никулина_И.А._гр.11ПТ1.doc

Имя компании: Пензенский гос. Университет

Тип документа: Прочее

Имя документа: Группа 11ПТ1 ВКР Никулина ИА

Дата проверки: 15.01.2017 23:39

Модули поиска: Интернет (Антиплагиат), Диссертации и авторефераты РГБ, Пензенский гос. Университет, Университетская библиотека онлайн, Модуль поиска ЭБС "Лань", Кольцо вузов, Модуль поиска ЭБС БиблиоРоссика

Текстовые статистики:

Индекс читаемости: очень сложный

Неизвестные слова: в пределах нормы

Макс. длина слова: в пределах нормы

Большие слова: в пределах нормы

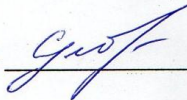
Оригинальные блоки: 75,14%

Заемствованные блоки: 24,86%

Заемствование из "белых" источников: 0%

Итоговая оценка оригинальности: 75,14%

16.01.2017 года



В.А. Сулов

