Министерство образования и науки Украины
Одесский национальный политехнический университет

На правах рукописи

Шапорин Владимир Олегович

УДК 004.056.5+004.413.4

МОДЕЛИ И МЕТОДЫ АНАЛИЗА РИСКОВ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Специальность 05.13.06 — Информационные технологии

Диссертация
на соискание научной степени
кандидата технических наук

Научный руководитель
Тишин Петр Метталинович
кандидат физико-математических
наук, доцент

Одеса — 2016

СОДЕРЖАНИЕ

СПИСОК УСЛОВНЫХ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

UI – нежелательный инцидент

TS – сценарий угрозы

НИ – нечеткий интеграл

НМ – нечеткая мера

ОМ – обращение Мебиуса

ИС – информационная система

ИБ – информационная безопасность

ТКС – телекоммуникационная система

АСАР – автоматизированная система анализа рисков

ВА – владелец актива

НМ – нечеткое множество

ЛП – лингвистическая переменная

ФП – функция принадлежности

СВ – структура влияния

ПО – программное обеспечение

ААА – аутентификация, авторизация, аудит

БЗ – база знаний

ВВХ – вероятностно-временные характеристики

ВВЕДЕНИЕ

Актуальность темы. В связи с конкурентной борьбой, деятельностью злоумышленников и вирусными атаками возрастает угроза информационной деятельности предприятий. С каждым годом растет сложность атак, появляются новые виды угроз, совершенствуются старые. Согласно отчетам 2015 года с Kaspersky lab, Dr. Web и SERT UA, Украина входит в ТОП-20 стран мира по уровню вирусной зараженности компьютеров. За этот период 58% корпоративных компьютеров подверглись хотя бы одной атаке из сети Интернет, причем осуществлялись эти атаки с использованием браузеров компьютеров (62%), приложений андроид (14%), приложений JAVA (13%) и др. В частности, атаки на бизнес-приложения выросли в три раза, по сравнению с прошлым периодом 2014 года.

В условиях развития киберпреступности важную роль приобретает безопасность систем и ресурсов (активов и их свойств), которая основывается на правилах и нормах, которые определяют действия при обнаружении инцидентов безопасности и сценариев, приводящих к ним и управления факторами угроз (места уязвимости системы). Все указанные элементы являются составными риска и определяют его характеристики в ходе реализации нарушение безопасности системы. Корректность и адекватность таких норм, в первую очередь, зависит от качества анализа рисков на этапе проектирования системы мер безопасности, который является наиболее затратным, как с финансовой точки зрения, так и с точки зрения затрат времени. В целях экономии средств, большинство организации не проводят анализ рисков ни на этапе проектирования или запуска информационной системы, ни периодически, в ходе ее функционирования. Такое отношение приводит к созданию угроз информационной безопасности системы и составляющим.

Существует два подхода к анализу рисков: первый – организация экспертной оценки проблемы с привлечением соответствующих специалистов по безопасности и заинтересованных лиц. Второй - использование автоматизированных систем анализа рисков для отдельных составляющих системы, или всей системы в целом, а также в произвольные моменты времени функционирования системы. В первом случае обеспечивается высокая достоверность оценки рисков, которая зависит от количества экспертов, однако работа экспертов связана с высокой оплатой труда и требует значительных временных затрат. Во втором случае используются традиционные математические и статистические методы, которые позволяют автоматизировать процесс анализа рисков, однако данные методы используют четкие параметры для описания элементов риска, что значительно снижает достоверность результатов.

Таким образом актуальной является разработка методов и моделей, основанных на теории нечетких множеств и нечетких чисел, позволит описывать параметры элементов риска в условиях неопределенности и повысить достоверность оценки рисков за счет нечетких функций агрегации.

Связь работы с научными программами, планами, темами. Диссертационная робота выполнялась у рамках госбюджетных научно-исследовательских работ: «Технології проектування, контролю і діагностики комп'ютерних систем та мереж» № 571-62, № госрегистрации 0107U001969, 2007-2010 р.р.; «Розробка засобів робочого і тестового контролю та діагностики обчислювальних систем і мереж» № 630-62, № госрегистрации 0108U001197, 2008-2009 р.р.; «Методи проектування та робочого діагностування складних цифрових систем і мереж» №37-62, № госрегистрации 0110U008194, 2011-2014 р.р.; «Методи проектування, аналізу інформаційних систем критичного застосування та їх компонентів» № 97-62, № госрегистрации 0114U005507, почалась у 2015р.

Цель и задачи исследования является повышение достоверности оценки рисков в задачах обеспечения защиты информационных систем, путем разра-

ботки моделей качественного и количественного оценивания процессов нарушения безопасности, а также методов анализа рисков.

Для достижения поставленной цели решены следующие задачи:

– проведен анализ существующих методов и моделей анализа рисков, используемых в области информационной безопасности;

– разработаны математические модели активов и инцидентов безопасности, с использованием нечеткого интеграла и нечетких мер;

– разработано семейство моделей сценариев угроз на основе нечетких временных сетей Петри;

– разработан метод оценки угроз с использованием нечеткого интеграла и нечетких мер для факторов воздействия;

– разработан метод оценки рисков на основе нечеткой классификации и правил принадлежности к соответствующим уровням риска;

– проведены практические испытания результатов исследования в лабораторных условиях и апробация на реальных объектах предпринимательства.

Объект исследования – процесс анализа и оценки рисков информационной безопасности в условиях неопределенности.

Предмет исследования – модели и методы анализа рисков информационной безопасности в условиях неопределенности.

Методы исследования. Метод лингвистической оценки активов, отношений и рисков основан на теории нечетких множеств. Классификация рисков основана на нечеткой кластеризации. Модели сценариев основаны на сетях Петри и нечетких базах знаний. Метод идентификации угроз основан на псевдоиерархических системах. Нечетка оценка элементов риска основана на использовании нечеткого интеграла.

Научная новизна состоит в развитии методов идентификации, анализа и оценки рисков информационной безопасности, которые используются при разработке систем защиты информационных ресурсов предприятий и при аудите рисков в процессе функционирования информационных систем, а именно:

– получил дальнейшее развитие метод оценки активов информационной системы, который, в отличие от существующих, описывает активы и их свойства в виде лингвистических переменных, что позволило давать качественную и количественную оценку при описании и ранжировании активов для процессов определения убытков данным активам;

– получили дальнейшее развитие модели сценариев угроз, которые отличаются описанием параметров ошибок, сбоев, отказов и атак на систему в виде нечетких переменных, что позволило повысить качество моделирования процессов возбуждения безопасности в условиях неопределенности и ограниченной информации;

– впервые разработан метод оценки угроз, который отличается иснаступлением предложенной множества нечетких мер для факторов угрозы и использованием нечеткого интеграла по нечеткой мере для оценки угроз, что позволило повысить точность оценки возникновения факторов нарушения безопасности;

– получил дальнейшее развитие метод лингвистической оценки рисков, который отличается использованием нечеткой классификации рисков, на основе кластеризации значений инцидентов и ущерба от них, что позволило повысить достоверность оценки рисков.

Практическая ценность полученных результатов. На основе результатов диссертационной работы разработана информационная технология, которая позволяет повысить достоверность оценки рисков и снизить вероятность ошибочных оценок. При использовании предложенной информационной технологии достоверность оценки риска составила 93% с вероятностью ошибки второго рода 0,04 соответственно. Разработана информационная технология была применена при проектировании информационных систем в ООО «Телекарт-Прибор», что позволило повысить достоверность оценки рисков на 7-11% и сократить время мониторинга рисков в среднем на 23%, что составляет 9 часов, в сравнении с 13 часами, в среднем, до внедрения информационной технологии.

Предложенные методы и модели внедрены в учебный процесс Одесского национального политехнического университета.

Личный вклад соискателя. В работах [7, 8, 11, 12, 13] автором исследовано идентификацию элементов риска, в частности активов, уязвимости и угроз. В работе [9] предложен общий подход к лингвистической оценки элементов риска. В работах [4, 5] предложен метод лингвистической оценки активов системы. В работах [1, 2, 3, 10] предложены модели сценариев с нечеткими параметрами. В работах [5, 14] предложен метод оценки угроз информационной безопасности. В работе [6] предложен метод лингвистической оценки рисков информационной безопасности.

Апробация результатов диссертации. Основные теоретические положения и результаты работы докладывались и обсуждались на 8, 12, 14 и 15 и Международных научно-практических конференциях «Современные информационные и электронные технологии» (Одесса, 2007, 2011, 2013, 2014) и семинара "Моделирование в прикладных научных исследованиях" (Одесса, 2015).

Публикации. Результаты исследований были представлены в 14 публикациях, среди которых 6 статей в научных журналах и сборниках научных трудов, определенных в МОН Украины как специальные издания по техническим наукам и 8 в материалах конференции и семинаров. Среди этих публикаций шестой изданиях, включенных в международных наукометрических баз Bielefeld Academic Search Engine (BASE), Российский индекс научного цитирования (РИНЦ), Index Copernicus Journals Master List.

РАЗДЕЛ 1. АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДЫ ИХ РАЗРЕШЕНИЯ

1.1 Современное состояние безопасности информационных систем

Любая информационная система предназначена для хранения и обработки информации, что позволяет автоматизировать бизнес процессы предприятия [1 – 4]. Деятельность предприятия направлена на получение прибыли и, соответственно, нарушение работы информационной системы может принести существенные финансовые, юридические и другие потери.

Информационная безопасность в информационных системах включает в себя широкий круг проблем при управлении ими [5 – 6]. Для благополучия бизнеса информационная безопасность имеет основополагающее значение и решает три основных задачи – обеспечение целостности, конфиденциальности и доступности ресурсов информационной системы [7 – 8, 14, 30].

1.1.1 Основные задачи в области информационной безопасности

Первой задачей является обеспечение целостности ресурсов. В условиях развития информационных систем, сегодня вся коммерческая информация, бухгалтерские данные, финансовая отчетность, клиентские базы, договора, новаторские идеи сотрудников фирмы, планы и стратегия её развития, хранятся в локальной информационно-компьютерной сети [4, 15, 18]. Далеко не всегда и не все документы дублируются на бумажных носителях, ибо объем информации очень велик. В таких условиях информационная безопасность предусматривает систему мер, которые призваны обеспечить надежную защиту серверов и рабочих станций от сбоев и поломок, ведущих к уничтожению информации или её частичной потере. Серьезный подход к данному вопросу означает, что информационная безопасность должна базироваться на профессиональном аудите всей IT-инфраструктуры фирмы. IT аудит позволяет провести оценку

состояния сети и оборудования, сделать анализ потенциальных угроз, выявить и вовремя устранить уязвимые места кабельной системы, серверных и рабочих станций, дисковых систем и нарушений в конфигурации оборудования. Таким образом, снижаются технические риски возможной потери информации.

К повреждению данных приводит и некорректная работа систем архивации, сетевого и прикладного ПО.

Обеспечение конфиденциальности информации связано с защитой коммерческих секретов [9, 11, 36], и напрямую влияет на конкурентоспособность фирмы и её устойчивость на рынке. Здесь информационная безопасность и защита сетей сталкивается с внешними и внутренними преднамеренными угрозами, направленными на хищение данных. Хакеры, промышленный шпионаж и утечка информации по вине собственных сотрудников представляют наибольшую угрозу. Соблазн продать ценную коммерческую информацию велик не только у увольняемых сотрудников, но и у тех, амбиции которых на рабочем месте неудовлетворенны. В данном случае, информационная безопасность принимает превентивные меры, направлены на контроль инсайдеров и многоступенчатую защиту серверов от внешних и внутренних атак.

Поэтому меры по противодействию несанкционированному доступу должны быть направлены на достижение двух целей:

– создавать условия, когда случайные или умышленные действия, приводящие к потере данных, становятся невозможны. Информационная безопасность решает эту проблему путем создания системы аутентификации и авторизации пользователей, разделения прав доступа к информации и контроля доступа.

– также важно создать систему, при которой сотрудники или злоумышленники не смогли бы скрыть совершенных действий. Здесь в помощь специалисту по ИБ приходит система контроля событий безопасности, аудит доступа к файлам и папкам.

Эффективными средствами защиты, как от внешних угроз, так и от внутренних, являются также [12]: введение системы паролей пользователей, приме-

нение для особо важной информации криптографических методов защиты (шифрование), ограничение доступа в помещения, применение индивидуальных цифровых ключей и смарт-карт, использование межсетевых экранов, установка систем защиты от утечек информации через электронную почту, FTP-серверы и Интернет-мессенджеры, защита информации от копирования.

В последнее время получили большое распространение такие способы взлома сетей, как распространение вредоносных компьютерных программ, выполняющих функции сбора и передачи информации (троянские программы), программ-шпионов [13, 17]. Для того, чтобы устранить подобные внешние риски, информационная безопасность предусматривает установку мощного антивирусного ПО и серверной защиты.

Информационная безопасность сети предполагает также защиту от атак извне, направленных на прекращение работоспособности серверов, компьютеров или компонентов сети. Речь идет о DDos-атак [45], попытках подбора паролей (bruteforce-атаки). Для защиты от подобных угроз информационная безопасность требует применения специального программного обеспечения – межсетевых экранов и систем проактивной защиты.

Обеспечение доступности информации для легитимных пользователей является одной из важнейших задач системных администраторов. Простои системы, в результате нарушения доступности часто приводят к финансовым и юридическим последствиям, потери репутации и доверия партнеров и клиентов.

1.1.2 Анализ компьютерных угроз

Согласно отчетам за 2015 год, опубликованных лабораторией Касперского, Dr. WEB и CERT UA (Computer Emergency Response Team of Ukraine – команда реагирования на компьютерные чрезвычайные события Украины) было выявлено следующее [16]:

– в 2015 году на 58% корпоративных компьютеров была отражена хотя бы одна атака вредоносного ПО, что на 3 п.п. больше, чем в прошлом году;

– 29% компьютеров, т.е. почти каждый третий компьютер в бизнес- среде, подверглись хотя бы одной атаке через интернет;

– при атаках на бизнес эксплойты к офисным приложениям используются в три раза чаще, чем в атаках на домашних пользователей;

– файловый антивирус сработал на 41% компьютеров корпоративных пользователей (детектировались объекты, обнаруженные на компьютерах или на съемных носителях, подключенных к компьютерам, — флешках, картах памяти, телефонах, внешних жестких дисках, сетевых дисках).

Основными целями атак было получение финансовой выгоды, как например операция Carbanak – APT-атака, при которой злоумышленники проникали в сеть банка-жертвы и искали критически важную систему, с помощью которой из атакованной финансовой организации выводили денежные средства. Всего по миру насчитывается более 100 жертв этой атаки, а суммарные убытки пострадавших организаций (в основном это были банки) могут достигать миллиарда долларов. Также целями злоумышленников была конфиденциальная информация. Среди пострадавших — юридические фирмы, инвестиционные компании, организации, работающие с криптовалютой Bitcoin, группы компаний и предприятия, вовлеченные в сделки слияния и поглощения, IT-компании, учреждения здравоохранения, риэлтерские компании, а также индивидуальные пользователи.

Анализ этих и других атак позволяет выделить несколько тенденций развития целевых атак на бизнес:

– под прицел злоумышленников попали организации, выполняющие различные операции с деньгами: банки, фонды и компании, связанные с биржами, в том числе с биржами криптовалют;

– атаки тщательно готовятся, злоумышленники исследуют интересы потенциальных жертв (сотрудников атакуемой компании) и выявляют сайты, которые они часто посещают, исследуют контакты жертвы, собирают информацию о поставщиках оборудования и услуг;

– собранные при подготовке атаки данные активно используются. Атакующие взламывают выявленные легитимные сайты, аккаунты пользователей из бизнес-контактов сотрудников атакуемой компании. Такие сайты/аккаунты используются в течение нескольких часов — с них распространяется вредоносный код, после чего заражение прекращается. Такая схема дает злоумышленникам возможность повторно использовать взломанный ресурс через несколько месяцев;

– активное использование подписанных файлов и легального ПО для сбора информации из атакованной сети;

– диверсификация атак, атаки на малый и средний бизнес;

Также отмечено, что общая статистика по корпоративным пользователям (география атак, рейтинг детектируемых объектов) в целом совпадает со статистикой по домашним пользователям. Это обуславливается тем, что бизнес-пользователи не существуют в изолированной среде, их компьютеры становятся объектами атак злоумышленников, которые распространяют вредоносные программы без учета специфики атакуемого. Таких атак/зловредов большинство, и данные по атакам, нацеленным именно на бизнес-пользователей, мало влияют на общую статистику.

В 2015 году при серфинге в интернете веб-атакам хотя бы раз подверглись 34,2% компьютеров пользователей интернета. В среднем уровень опасности интернета за год снизился на 4,1 п.п. Данный тренд плавного снижения начался в 2014 году, и продолжается второй год подряд.

Всего в 2015 году было зафиксировано около 4 миллионов вредоносных и потенциально нежелательных программ. Это в два раза больше, чем в прошлом году. При этом, как правило, риску подвержены личные устройства пользователей и съемные накопители.

На основе анализа статистики мы можем выделить основные направления развития деятельности киберкриминала:

– часть людей, занимавшихся киберкриминальной деятельностью, стремится минимизировать риски уголовного преследования и переключается с атак вредоносных программ на агрессивное распространение рекламного ПО;

– в используемом в массовых атаках ПО растет доля относительно несложных программ. Такой подход позволяет злоумышленникам быстро обновлять вредоносное ПО, чем и достигается эффективность атак;

– злоумышленники освоили не-Windows платформы – Android и Linux: для этих платформ созданы и используются практически все виды вредоносных программ;

– в ходе своей деятельности киберкриминал активно использует современные технологии анонимизации – Tor для сокрытия командных серверов и Биткойны для проведения транзакций.

Все большая доля срабатывания антивируса приходится на «серую зону»: в первую очередь это различные рекламные программы и их модули. В нашем рейтинге веб-угроз 2015 года представители этого класса программ занимают двенадцать позиций в TOP 20. В течение года рекламные программы и их компоненты были зафиксированы на 26,1% всех компьютеров пользователей, на которых сработал наш веб-антивирус. Увеличение количества рекламных программ, агрессивные способы их распространения и их противодействие детектированию антивирусов продолжают тренд 2014 года. Распространение такого ПО приносит немалые деньги, и его создатели в погоне за наживой иногда используют приемы и технологии, характерные для вредоносных программ.

В 2015 году у вирусописателей выросла популярность эксплойтов для Adobe Flash Player. По нашим наблюдениям, лэндинг-страницы с эксплойтами чаще всего загружают именно эксплойты к Adobe Flash Player. Это можно объяснить двумя причинами: во-первых, в течение года было найдено большое количество уязвимостей в данном продукте. Во-вторых, в результате утечки данных от Hacking Team в публичном доступе оказалась информация_о неизвест-

ных ранее уязвимостях во Flash Player, чем и воспользовались злоумышленники.

В 2016 году ожидается продолжения развития шифровальщиков, нацеленных на не-Windows платформы: увеличение доли Android и появление шифровальщиков, нацеленных на Mac OS. Учитывая, что Android активно используется и в бытовой электронике, могут произойти и первые атаки крипторов на «умные» устройства.

1.2 Основные угрозы информационной безопасности

Согласно стандартам по менеджменту рисков и информационной безопасности, угрозой является возможность наступления инцидента безопасности в информационной системе [44]. Под этим термином понимаются некоторые события и источники их возникновения. Однако, при описании и моделировании данных событий, редко уделяется должное внимание описанию и определению условий, при которых данные события способны возникнуть и развиваться. Исходя из этого, целесообразно разделить это понятие на два – угрозы и сценарии угроз. Первый описывает источник событий и условия его возникновения, второй собственно те действия, которые этим источником вызываются.

Существует множество классификаций угроз информационной безопасности, которые разделяют угрозы по таким признакам как источник угрозы, тип угрозы, тип воздействия и многие другие [46]. Однако существует несколько типов классификации, которые являются основными в современных стандартах по информационной безопасности и наиболее часто используются в научной литературе.

По расположению источника угрозы делят на внутренние и внешние угрозы. Внутренние угрозы предполагают нахождение источника угрозы внутри информационной системы или ее коммуникационной структуры. Основными угрозами, подходящими под данную классификацию являются:

– пользователи системы. Неверные действия, вызванные неосторожностью или незнанием, могут привести к возникновению уязвимости системы;

– обслуживающий персонал системы. Администраторы, инжинеры, программисты и другие технические сотрудники, в следствии недостаточной квалификации или ошибки, могут оставить уязвимые места в системе или создать новые;

– инсайдеры. Любой из сотрудников предприятия, имеющий в той или иной степени доступ к системе, может намеренно осуществлять вредоносную деятельность по причине недовольства, обиды, подкупа или иной мотивации;

– информационная система. Нечастый случай, когда алгоритмы работы системы способствуют возникновению уязвимых мест или инцидентов, приводящих к нарушению безопасности.

Внешние угрозы предполагают воздействие на информационную систему извне. Для осуществления внешней угрозы необходимы определенные предпосылки – наличие уязвимости [51, 52, 57, 58] в информационной системе, мотивация к совершению нарушения безопасности и другие. Внешние угрозы:

– вирусы. Специальные программы, действия которых осуществляются в трех основных направлениях: создание условий, препятствующих нормальной работе информационной системы, полная блокировка работы информационной системы, поиск и использование уязвимых мест системы для открытия удаленного доступа к ней;

– злоумышленники (хакеры) – человек или группа людей, которые воздействуют на систему с целью получения материальной или иной выгоды;

– техногенные, природные и другие катаклизмы. Воздействие внешних систем, окружающей среды и иных факторов, приводящие к нарушению работоспособности системы.

Данный список не претендует на полноту описания всех возможных угроз, однако дает представление о наиболее распространенных из них.

По характеру возникновения угрозы делятся на непреднамеренные и преднамеренные угрозы. Под непреднамеренными угрозами понимаются те, которые возникают в результате совпадения некоторых событий, и приводят к нарушению безопасности системы. Если проводить параллель с предыдущей классификацией, случайными угрозами можно назвать всей пользователей системы и различные катаклизмы, а также, иногда, вирусы.

Преднамеренные угрозы предполагают воздействие на систему с определенной целью, которая осознана и четко понимается. Как правило, данные угрозы описывают определенный умысел в действиях, такой как финансовая выгода, блокировка или уничтожение системы, месть и т. д.

Преднамеренные угрозы, в большинстве случаев, можно спрогнозировать, опираясь на соответствующие статистические данные, характер деятельности предприятия, конкурентные ожидания и пр. Непреднамеренные угрозы, в силу случайного характера их возникновения, наоборот достаточно сложно определить в полной мере, так как они описывают возможность ошибки, сбоя и другие единичные случаи, которые не поддаются систематизации.

Все угрозы приводят к определенным действиям, которые вызывают инциденты безопасности путем осуществления де. Такими действиями являются атаки на систему, ошибки пользователей и администраторов, сбои и отказы системы. Данные действия далее будем называть сценарии, которые описывают последовательность действий, приводящих к инцидентам безопасности.

1.2.1 Воздействие внутренних угроз на процессы нарушения безопасности

Среди множества существующих сценариев, существуют группы наиболее типичных для внутренних угроз, которые наиболее часто происходят в различных информационных системах [8, 10, 17, 23, 61, 62].

Почтовые системы. Использование почты несет потенциальный риск для информационной системы. Во-первых, сами почтовые системы на сегодняшний день не обладают достаточно широким функционалом по безопасности. Во-вторых, почтовые программы, позволяющие управлять несколькими почтовы-

ми ящиками, несут опасность на протокольном уровне, и, несмотря на удобство, также снижают уровень безопасности. Третье, и главное, неосторожная работа с корреспонденцией может привести к заражению компьютеров в сети и обходу систем безопасности (чтение подозрительных писем из не проверенных источников и др.).

Интернет серфинг. Опасности использования web-страниц заключаются в том, что на них могут размещаться потенциально опасные ссылки на загрузку вирусов, переход на другие опасные сайты и т. д. Неосторожное использование поисковых систем и web-страниц, также способствует возникновению уязвимых мест и очень опасно для безопасности информационной системы.

Проблема открытых окон и столов. Ввод паролей в открытом виде, записывание идентификационных данных в доступных местах, оставление рабочего места с активированной учетной записью и другие распространенные ошибки пользователей приводят к хищению и неправомерному использованию этих данных сторонними лицами.

Компьютерная грамотность. Пользователи зачастую не имею достаточных знаний в области безопасного использования информационной системы, что приводит к созданию уязвимых мест, в частности, для вирусов и другого злонамеренного кода. Также, недостаточная квалификация инженерного персонала может обуславливать ошибки в настройках оборудования, сервисов, алгоритмов работы системы, что приводит к низкому уровню защищенности системы.

Социальная инженерия. Относительно новый способ нарушения безопасности, связанный с предыдущей проблемой. Заключается в создании ситуаций, когда человек добровольно разглашает свои идентификационные данные (социальный опрос, подмена страниц ввода данных и др.)

Использование личных устройств. Распространенная в последнее время тенденция к использованию на рабочем месте личных устройств (ноутбуки, планшеты, смартфоны и т.д.) приводит к снижению уровня безопасности, в свя-

зи с функционированием этих устройств вне защищаемой системы и повышению риска заражения вирусами, кражи идентификационных данных и пр.

Все эти, а также многие другие, способы нарушения безопасности трудно поддаются анализу рисков, в связи со случайным характером возникновения. Наиболее оптимальным способом анализа данных проблем является определение инцидентов, которые могут быть вызваны внутренними угрозами с целью дальнейшего принятия решения об уровне риска от них и мерах по его обработке.

1.2.2 Воздействие внешних угроз на процессы нарушения безопасности

Внешние угрозы, как правило, характеризуются намеренными действиями, приводящими к нарушению работы информационной системы. Такие действия, как правило, мотивированы недовольством действиями организации, желанием отомстить за что либо, промышленным шпионажем или намерением продемонстрировать свои возможности [47 – 48]. Намеренные атаки на информационную систему и ее ресурсы нацелены на нарушение трех основных свойств активов.

Вирусная активность. Распространение вирусов наблюдается во всех сферах информационной деятельности. Как показывает анализ данной проблемы, выделяются два основных направления вирусной деятельности в компьютерных системах:

– блокирование информационной системы или ее компонентов. Осуществление заражения устройств и носителей информации вирусами, которые приводят к затруднению или невозможности работы объектов заражения с целью шантажа или уничтожения корпоративной информации ;

– создание скрытых входов в систему или скрытой передачи информации из системы. Заражение системы, которое позволяет злоумышленникам получать доступ к информационной системе или ее компонентам, или красть идентификационную или конфиденциальную информацию.

Деятельность злоумышленников. Данная деятельность связана с намеренным причинением ущерба деятельности организации. Среди атак от злоумышленников можно выделить следующие направления:

– финансовая выгода. Осуществление атак, которые приводят к блокированию работы системы или учетных записей пользователей с целью вымогательства и шантажа (отказ в обслуживании, подмена доверенного объекта и пр.).

– заказные атаки. Кража конфиденциальной информации, которая может пригодиться в деятельности корпоративных конкурентов (прогнозные отчеты, статистические данные, ценные бумаги, криптовалют и т. д.) или снизить конкурентоспособность предприятия в своей сфере деятельности;

– протест. Осуществление атак в знак протеста против деятельности предприятия или политических, моральных и других взглядов.

На сегодняшний день наибольшую популярность приобрели атаки типа отказ в обслуживании (Deny of Service, DoS), которые нацелены на нарушение доступности системы или ее компонент. Данный тип атак применяется по разным причинам – от простого доказательства своих способностей хакером, до намеренных действий против конкретной организации. Все остальные виды атак имеют частный характер в рамках промышленного шпионажа или атак на конкретные частные лица. В любом случае, анализируя деятельность организации, ее информационно-телекоммуникационную структуру, возможно предусмотреть большую часть предполагаемых угроз и применить соответствующие меры безопасности.

1.3 Современные методы анализа рисков информационной безопасности

При построении комплексной системы защиты информационно системы, наиболее важным и первоочередным этапом является изучение деятельности предприятия и ее целей [39, 42]. Это дает возможность определить, что именно

необходимо защитить, какой уровень угрозы допустим и, исходя из этого, способы обеспечения безопасности.

Для обеспечения данного этапа существует множество методов, которые позволяют оценить уровень риска для деятельности предприятия, в том числе и для информационной безопасности [27, 37]. Большинство этих методов базируются на соответствующих европейский и отечественных стандартах, которые позволяют определить базовые подходы к обеспечению безопасности, терминологию в данной области и рекомендации по их использованию.

1.3.1 Базовые понятия анализа рисков

Учитывая специфику предметной области, а именно соседство таких сфер деятельности как экономическая деятельность, инженерная деятельность, документоведение и другие, в области анализа и управления рисками сложилась специфическая терминологическая база, в применении которой зачастую происходит путаница. Основными терминами при анализе рисков являются:

– *информационная безопасность*. Свойство информации сохранять целостность, конфиденциальность и доступность;

– *оценка риска*. Общий процесс идентификации, анализа и оценивания риска;

– *идентификация риска*. Процесс обнаружения, распознавания и описания рисков;

– *анализ риска*. Систематическое использование информации для определения источников риска и их оценивания;

– *активы*. Все что имеет ценность для организации. Понимаются как ресурсы системы, так и их свойства;

– *инцидент информационной безопасности*. Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или безопасность;

– *Риск*. Влияние неопределенности на цели;

– *Вероятность, возможность*. Шанс того, что что-то может произойти;

Основной задачей при анализе рисков является оценить уровень риска, который определяется исходя из вероятности возникновения инцидента и последствий от этого инцидента. В общем случае процесс анализа рисков состоит из следующих этапов:

1. Определить ценность информационных активов и провести соответствующее ранжирование.
2. Оценить потенциальный ущерб от реализации каждой угрозы в отношении каждого информационного актива.
3. Определить вероятность реализации каждой из угроз ИБ.
4. Определить общий потенциальный ущерб от каждой угрозы в отношении каждого актива за контрольный период (за один год).
5. Провести анализ полученных данных по ущербу для каждой угрозы.
6. По каждой угрозе необходимо принять решение: принять риск, снизить риск либо перенести риск:
   – принять риск – значит осознать его, смириться с его возможностью и продолжить действовать как прежде. Применимо для угроз с малым ущербом и малой вероятностью возникновения;
   – снизить риск – значит ввести дополнительные меры и средства защиты, провести обучение персонала и т д. То есть провести намеренную работу по снижению риска. При этом необходимо произвести количественную оценку эффективности дополнительных мер и средств защиты. Все затраты, которые несет организация, начиная от закупки средств защиты до ввода в эксплуатацию (включая установку, настройку, обучение, сопровождение и проч.), не должны превышать размера ущерба от реализации угрозы;
   – перенести риск – значит переложить последствия от реализации риска на третье лицо, например с помощью страхования.

Риск может быть оценен двумя способами – качественно и/или количественно.

В результате количественной оценки рисков должны быть определены:

– ценность активов в денежном или другом выражении;

– полный список всех угроз ИБ с ущербом от разового инцидента по каждой угрозе;

– частота реализации каждой угрозы;

– потенциальный ущерб от каждой угрозы;

– рекомендуемые меры безопасности, контрмеры и действия по каждой угрозе.

При качественном подходе не используются количественные или денежные выражения для объекта оценки. Вместо этого, объекту присваивается показатель, проранжированный по определенной лингвистической или бальной шкале. Для сбора данных при качественной оценке рисков применяются опросы целевых групп, интервьюирование, анкетирование, личные встречи. Анализ рисков информационной безопасности качественным методом должен проводиться с привлечением сотрудников, имеющих опыт и компетенции в той области, в которой рассматриваются угрозы.

1. Определить ценность информационных активов. Ценность актива можно определить по уровню критичности (последствиям) при нарушении характеристик безопасности (конфиденциальность, целостность, доступность) информационного актива или его важности.

2. Определить вероятность реализации угрозы по отношению к информационному активу. Для оценки вероятности реализации угрозы может использоваться трехуровневая качественная шкала (низкая, средняя, высокая).

3. Определить уровень возможности успешной реализации угрозы с учетом текущего состояния ИБ, внедренных мер и средств защиты. Для оценки уровня возможности реализации угрозы также может использоваться трехуровневая качественная шкала (низкая, средняя, высокая). Значение возможности реализации угрозы показывает, насколько выполнимо успешное осуществление угрозы.

4. Сделать вывод об уровне риска на основании ценности информационного актива, вероятности реализации угрозы, возможности реализации угрозы. Для определения уровня риска можно использовать пятибалльную или десятибалльную шкалу. При определении уровня риска можно использовать эталонные таблицы, дающие понимание, какие комбинации показателей (ценность, вероятность, возможность) к какому уровню риска приводят.

5. Провести анализ полученных данных по каждой угрозе и полученному для нее уровню риска. Часто группа анализа рисков оперирует понятием «приемлемый уровень риска». Это уровень риска, который компания готова принять (если угроза обладает уровнем риска меньшим или равным приемлемому, то она не считается актуальной). Глобальная задача при качественной оценке — снизить риски до приемлемого уровня.

6. Разработать меры безопасности, контрмеры и действия по каждой актуальной угрозе для снижения уровня риска.

Оба способа имеют свои положительные и отрицательные стороны, и на практике более адекватным является комбинированная оценка элементов риска. При этом возможно использовать лингвистические переменные с термами, отражающими качественную оценка элемента, а благодаря семантическим правилам иметь возможность преобразовать терм в количественное значение.

1.3.2 Классификация методов анализа рисков

Строгой классификации для методов анализа рисков не существует, однако существуют различия в подходах к анализу рисков, способах представления элементов риска, функциональных возможностях и пр. На основе таких различий можно выделить три основных группы – графические, математические и лингвистические методы.

Графические методы [49 – 50]. Многие методы предусматривают визуализацию объектов анализа и процессов взаимодействия между ними. При этом строятся графы, деревья или диаграммы, позволяющие различным способом отображать информацию об исследуемых объектах. В большинстве случаев

данные методы позволяют осуществить лишь идентификацию элементов риска и способы взаимодействия между ними.

Математические методы [31, 33]. Методы, которые предусматривают определение свойств объектов и их взаимодействия при помощи некоторых формальных языков описания, определяющих законы функционирования, изменения свойств и пр. Данные методы позволяют не только идентифицировать элементы, но и анализировать их поведение, изменение их свойств и влияние на другие элементы.

Лингвистические методы [50]. Данный класс методов наиболее популярен и прост в использовании, однако не всегда способен привести к адекватной оценке ситуации. Данные методы не предусматривают каких-либо инструментальных средств и программ, и требуют лишь наличия команды лиц, ответственных за анализ риска. При этом все этапы оценки риска, на сколько это возможно, предполагают только устное общение между группой лиц, в ходе которого идентифицируются элементы риска, строятся предположения о их поведении и осуществляется приблизительная оценка возможностей и ущербов.

Количество методов, которые способны обеспечить весь цикл анализа рисков, достаточно мало и такие методы, как правило, дорогостоящи в применении. Другие методы требуют привлечения значительного количества экспертов в различных областях, таких как информационные технологии, экономика, законодательство, что также значительно увеличивает стоимость проведения анализа рисков.

Наравне с этим, в последнее время, достаточно интенсивно развиваются методы анализа и оценки риска, которые основаны на элементах нечеткой логики. Такие методы представлены, например, в [28 – 29, 40 – 41] и позволяют значительно расширить возможности математических методов анализа рисков.

1.3.3 Графические методы анализа

Анализ дерева событий (Event-tree-analysis, ETA) – является логическим метод моделирования для успеха так и для неудачи, исследующий ответ через

событие и инициирует генерацию пути для оценки вероятностей исходов и общего системного анализа.

Общая цель анализа дерева событий - определение вероятности возникновения возможных негативных последствий, которые могут причинить вред системе, из выбранного исходного события. Для этого необходимо использовать подробную информацию о системе, чтобы понять промежуточные события, сценарии аварий, и используя исходные события построить диаграмму событий. Дерево событий начинается с инициирующего события, где последствия этого события следуют в двоичным образом. Каждое событие создает путь для которого может быть рассчитана общая вероятность наступления этого пути.

Анализ видов и последствий отказов (Failure mode and effects analysis, FMEA). Первоначально разработанный и опубликованный военно-промышленным комплексом США (в форме стандарта MIL-STD-1629), анализ видов и последствий отказов является сегодня таким популярным, поскольку в некоторых отраслях промышленности разработаны и опубликованы специализированные стандарты, посвященные FMEA. Прежде всего, должны быть четко определены границы рассматриваемой системы. Система может представлять собой техническое устройство, процесс или что угодно еще, подверженный FMEA-анализу. Далее идентифицируются виды возможных отказов, их последствия и возможные причины возникновения. В зависимости от размера, природы и сложности системы определения видов возможных отказов может быть выполнено для всей системы в целом или для каждой ее подсистемы индивидуально. В последнем случае последствия отказов на уровне подсистемы будут проявляться, как виды отказов на уровень выше. Идентификация видов и последствий отказов должна быть выполнена методом «снизу-вверх», до достижения верхнего уровня системы. Для характеристики видов и последствий отказов, определенных на верхнем уровне системы, используются такие параметры, как интенсивность, критичность отказов, вероятность возникновения и т.п. Эти параметры могут быть либо рассчитаны «снизу-вверх» с нижних уровней системы, или явно заданные на ее верхнем уровне. Эти параметры могут носить

как количественный, так и качественный характер. В результате для каждого элемента системы верхнего уровня рассчитывается своя уникальная мера, исчисляется из этих параметров по соответствующим алгоритмом. В большинстве случаев эту меру называют «коэффициентом приоритетности риска», «критичностью», «уровнем риска» или другим подобным образом.

Метод анализа дерева решений позволяет последовательно представить альтернативные варианты решений с их выходными данными и соответствующей неопределенностью. Как и при выполнении анализа дерева событий, построение следует начинать с начального события или принятого решения. Далее необходимо построить пути развития событий, определить результаты, которые могут быть получены при реализации событий, и различные решения, которые могут быть приняты. Построение дерева решений начинают с начального решения, например решения о возобновлении проекта А или проекта В. Поскольку могут быть реализованы два гипотетических проекта, то далее могут произойти соответствующие события и могут быть приняты различные решения. Этот процесс представляют в форме дерева по аналогии с деревом событий. Вероятность событий может быть оценена вместе с оценкой затрат и/или эффективности окончательного результата выбранного пути развития событий. Информация, касающаяся наилучшего пути принятия решений, имеет логическую форму, следовательно, возможен расчет наибольшего среднего значения, рассчитанного как произведение всех условных вероятностей на данном пути принятия решений на значение полученного результата.

Методология CORAS. Методология разработана в рамках программы Information Society Technologies. Ее суть заключается в адаптации, уточнении и комбинировании таких методов проведения анализа рисков, как event-tree-analysis, цепи Маркова, Fazop и Fmea. Метод CORAS использует модель UML. Для документирования промежуточных результатов и для того, чтобы представить полные заключения об анализе рисков информационной безопасности, используются специальные диаграммы CORAS, которые встроены в UML. Все работы по определению рисков проводятся с помощью следующих процедур:

– подготовительные мероприятия - сбор общих сведений об объекте анализа;

– представление клиентом объектов, которые необходимо проанализировать;

– детализированное описание задачи аналитиком;

– проверка корректности и полноты документация, представленной для анализа;

– мероприятия по выявлению рисков, (осуществляется, например, в форме семинара) возглавляемые аналитиками;

– оценка вероятностей и последствий инцидентов информационной безопасности;

– выявление приемлемых рисков и рисков, которые должны быть представлены на дальнейшую оценку для возможного устранения;

– устранения угроз, с целью сокращения вероятности и / или последствий инцидентов в области информационной безопасности.

1.3.4 Математические методы анализа

Анализ влияния человеческого фактора. Метод HRA применяют для оценки влияния действий человека, в том числе ошибок оператора, на работу системы. Во многих процессах существует возможность ошибки оператора, особенно в случае если у оператора недостаточно времени для принятия решений. Вероятность того, что события будут развиваться таким образом, что приведут к серьезным проблемам, должна быть мала. Тем не менее в некоторых случаях действие оператора может быть единственной защитой, предотвращающей катастрофические последствия отказа. Значимость оценки действий оператора подтверждается происшествиями, в которых критические ошибки оператора способствовали катастрофическому развитию событий. Эти происшествия показывают неприемлемость оценок риска, учитывающих только технические и программные средства системы. Они показывают опасность игнорирования ошибок оператора. Более того, оценка действий оператора позволяет

выявить ошибки, которые могут отрицательно влиять на производительность, и определить способы устранения данных ошибок и других отказов (технических и программных средств).

Процесс HRA включает следующие этапы:

– постановка задачи. Определение типов действий оператора (человека), которые должны быть исследованы и оценены;

– анализ задачи. Определение способов выполнения задачи и вспомогательных средств, необходимых для ее выполнения;

– анализ ошибки оператора. Определение отказов, возникающих в процессе выполнения задачи, возможных ошибок оператора и способов их устранения;

– представление. Определение того, как эти ошибки при выполнении задачи в сочетании с другими событиями, связанными с оборудованием, программным обеспечением и воздействующими факторами, могут быть использованы для расчета вероятности отказа системы в целом.

– предварительная проверка. Определение ошибок или задач, требующих детальной количественной оценки.

– количественная оценка. Определение вероятности ошибок оператора и отказов при выполнении задачи.

– оценка воздействия. Определение значимости ошибок или задач, т. е. ошибок и задач, в большей степени влияющих на обеспечение надежности или приемлемого уровня риска.

– сокращение ошибок. Определение способов сокращения количественных ошибок оператора.

– документирование. Определение информации и деталей анализа HRA, которые должны быть зарегистрированы.

На практике процесс HRA чаще всего выполняют поэтапно, хотя иногда некоторые его части (например, анализ задач и идентификацию ошибок) проводят параллельно.

Марковский анализ применим в ситуации, когда будущее состояние системы зависит только от ее текущего состояния. Данный метод обычно используют для анализа ремонтопригодных систем, которые могут работать во многих режимах, и в ситуациях, когда применение анализа надежности отдельных блоков системы нецелесообразно. Метод может быть применен к более сложным системам, используя более высокий порядок процессов Маркова, и ограничен только моделью, математическими вычислениями и предположениями. Процесс марковского анализа является количественным методом и может быть дискретным (использование вероятностей перехода между состояниями) или непрерывным (использование коэффициентов интенсивности перехода из состояния в состояние). Марковский анализ может быть выполнен вручную, однако характеристики метода позволяют использовать для него компьютерные программы. Марковский анализ основан на понятии «состояния» (например, работоспособное и неработоспособное состояния) и перехода между этими состояниями во времени в предположении постоянной вероятности перехода. Стохастическую матрицу вероятностей перехода используют для описания переходов между состояниями и необходимых вычислений.

Метод Монте-Карло. Метод может быть применен в сложных ситуациях, которые трудны для понимания и решения с помощью аналитических методов. Модели систем могут быть разработаны с использованием таблиц и других традиционных методов. Однако существуют и более современные программные средства, удовлетворяющие высоким требованиям, многие из которых относительно недороги. Если модель разрабатывают и применяют впервые, то необходимое для метода Монте-Карло количество итераций может сделать получение результатов очень медленным и трудоемким. Однако современные достижения компьютерной техники и разработка процедур генерации данных по принципу латинского гиперкуба позволяют сделать продолжительность обработки незначительной во многих случаях. Процесс включает следующие этапы:

– определение модели или алгоритма, которые наиболее точно описывают поведение исследуемой системы;

– многократное применение модели с использованием генератора случайных чисел для получения выходных данных модели (моделирование системы). При необходимости моделируют воздействие неопределенности. Модель записывают в форме уравнения, выражающего соотношение между входными и выходными параметрами. Значения, отобранные в качестве входных данных, получают исходя из соответствующих распределений вероятностей, характеризующих неопределенности данных.

С помощью компьютера многократно используют модель (часто до 10000 раз) с различными входными данными и получают выходные данные. Они могут быть обработаны с помощью статистических методов для получения оценок среднего, стандартного отклонения, доверительных интервалов.

Байесовский анализ. Байесовский анализ отличается от классической статистики предположением, что параметры распределений являются не постоянными, а случайными переменными. Вероятность Байеса можно легко понять, если рассматривать ее как степень уверенности в определенном событии в противоположность классическому подходу, основанному на объективных свидетельствах. Поскольку подход Байеса основан на субъективной интерпретации вероятности, то он может быть полезен при выборе решения и разработке сетей Байеса (или сетей доверия). Сеть Байеса представляет собой графическую модель, представляющую переменные и их вероятностные взаимосвязи. Сеть состоит из узлов, представляющих случайные переменные, и стрелок, связывающих родительский узел с дочерним узлом.

1.3.5 Лингвистические методы

Метод мозгового штурма. Метод мозгового штурма представляет собой обсуждение проблемы группой специалистов в дискуссионной манере, целью которого является идентификация возможных видов отказов и соответствующих опасностей, риска, критериев принятия решений и/или способов обработки риска. Термин «мозговой штурм» часто используют более широко для обозначения любого обсуждения в группе. Однако в процессе классического мозгового штурма применяют специальные методы, когда утверждения одних участни-

ков обсуждения способствуют возникновению у остальных участников мозгового штурма новых оригинальных идей. Метод предполагает стимулирование обсуждения, периодическое направление обсуждения группы в смежные области и обеспечение охвата проблем, выявленных в результате обсуждения.

Процесс мозгового штурма может быть формальным или неформальным. Формальный процесс мозгового штурма обычно более структурирован: участники заранее подготовлены, точно установлены цель обсуждения и способы оценки выдвинутых идей и полученных результатов. Неформальный процесс мозгового штурма менее структурирован и часто носит узкоспециализированный характер.

Структурированные или частично структурированные интервью. В структурированном интервью опрашиваемому задают вопросы из заранее подготовленного перечня, поощряющие всесторонний анализ ситуации и, таким образом, более полную идентификацию опасностей и риска. Частично структурированное интервью аналогично структурированному, однако оно обеспечивает большую свободу при обсуждении исследуемой проблемы. Вначале необходимо составить перечень вопросов, направляющих размышления опрашиваемого. Вопросы должны быть, насколько возможно, простыми, изложены на понятном для опрашиваемого языке и охватывать только одну проблему. Ответы на вопросы не должны быть ограничены по времени. Возможные последующие вопросы, направленные на разъяснение ответов, должны быть подготовлены заранее. Затем вопросы должны быть предложены опрашиваемому лицу. При уточнениях ответы должны быть ограничены по времени. Необходимо следить за тем, чтобы постановка вопроса не подсказывала опрашиваемому определенный ответ. При анализе ответов необходимо проявлять гибкость и обеспечить возможность исследования областей, предлагаемых опрашиваемыми в своих ответах.

Контрольные листы. Контрольные листы представляют собой перечни опасностей, риска или отказов средств управления, которые обычно разрабатывают на основе полученного ранее опыта, результатов предыдущей оценки рис-

ка или результатов отказов, произошедших в прошлом. Должна быть выполнена следующая процедура:

– определение области применения;

– составление контрольного листа таким образом, чтобы он охватывал всю область применения. Контрольные листы должны быть тщательно составлены для достижения поставленной цели. Например, составленный ранее контрольный лист не может быть использован при идентификации новых опасностей или риска;

– лицо или группа лиц должны применять контрольный лист последовательно к каждому элементу процесса или системы для определения того, представлен ли этот элемент в контрольном листе.

Структурированный анализ сценариев методом «что, если?» (SWIFT). Метод SWIFT первоначально был разработан в качестве более простой альтернативы исследования HAZOP. Это систематизированный метод исследования сценариев, основанный на командной работе, в котором используют набор слов или фраз-подсказок, помогающих в процессе совещания участникам группы идентифицировать опасные ситуации и создать сценарий их развития. Ведущий и группа, используя стандартные фразы «что, если» в сочетании с подсказками исследуют, как система или организация будут вести себя под воздействием опасного события. Метод SWIFT обычно применяют для больших систем с более высоким уровнем детализации, чем позволяет исследование HAZOP.

1.4 Выводы

В ходе обзора ситуации в области информационной безопасности, анализа современных методов обеспечения безопасности и анализа рисков, было определено следующее:

– с каждым годом растет число вредоносного программного обеспечения. Увеличивается количество вирусных атак и способов их применения. Украина входит в число стран с наибольшей вирусной и хакерской активностью;

– выявлены основные угрозы информационной безопасности и процессы, которые ими инициируются;

– выявлено, что основным способом обеспечения безопасности является анализ информационной системы на наличие рисков нанесения ущерба имеющимся ресурсам;

– определены основные элементы риска, идентификация которых необходима для достоверного анализа рисков и адекватного принятия решений об уровне риска;

– рассмотрены наиболее распространенные методы анализа рисков, определены способы решения задач в этих методах.

Рассмотрев существующие методы анализа рисков можно увидеть, что основными проблемами в их применении являются:

– высокие финансовые затраты на осуществление анализа рисков;

– необходимость привлечения большого количества экспертов;

– отсутствие у многих методов возможности проведения полного цикла оценки рисков;

– отсутствие у многих методов возможности учета случайных и неполных событий.

Беря во внимание данные проблемы, можно сформулировать следующие требования к современным методам анализа рисков:

– минимизация количества задействованных экспертов в процессе анализа рисков;

– использование моделей и методов, которые позволяют учитывать неполноту или отсутствие части информации о функционировании системы.

РАЗДЕЛ 2.
ИДЕНТИФИКАЦИЯ ЭЛЕМЕНТОВ РИСКА.
МОДЕЛИ АКТИВОВ И ИНЦИДЕНТОВ.

2.1 Применение современных инструментальных и математических средств в анализе рисков

2.1.1 Диаграммы Coras

Одним из ближайших, к рассмотренным стандартам по информационной безопасности и менеджменту рисков, методов является Coras [37]. Данный метод основывается на графическом представлении элементов риска при помощи диаграмм активов, угроз и рисков. Диаграмма активов позволяет определить все активы системы и отношения между ними. Данный тип диаграмм удобен при выявлении активов на начальном этапе анализа и используется в далее в работе. Диаграммы угроз позволяют выявлять элементы риска, которые могут повлиять на ущерб активам, а также различные типы отношений между этими элементами. Пример такой диаграммы для угрозы «злоумышленник» представлен на рисунке 2.1.

Данная диаграмма описывает взаимодействие выявленных следующих элементов риска:

Угрозы: H;

Сценарии угроз: HSS – злоумышленник запустил на сервере свои сценарии, HSP – злоумышленник похитил ключи и логины пользователей, HSD – злоумышленник провел DoS атаку на шлюз, HPA – злоумышленник обошел правила доступа к сегментам сети, HPG – злоумышленник обошел правила доступа на шлюзе;

Нежелательные инциденты: HAN – злоумышленник прорвал защиту шлюзов и имеет доступ в корпоративную сеть, HAS – злоумышленник получил доступ к серверам, что может повлиять на их работу или доступность, HAG – злоумышленник получил доступ к специализированным сегментам сети или периферийным устройствам системы, UDO – злоумышленник смог получить в пользование логины и пароли легальных пользователей системы, NAB – нарушена доступность сети, в результате атак злоумышленника, HAR – злоумышленник имеет доступ к управлению сервисов системы, HAD – злоумышленник имеет доступ к корпоративным данным;

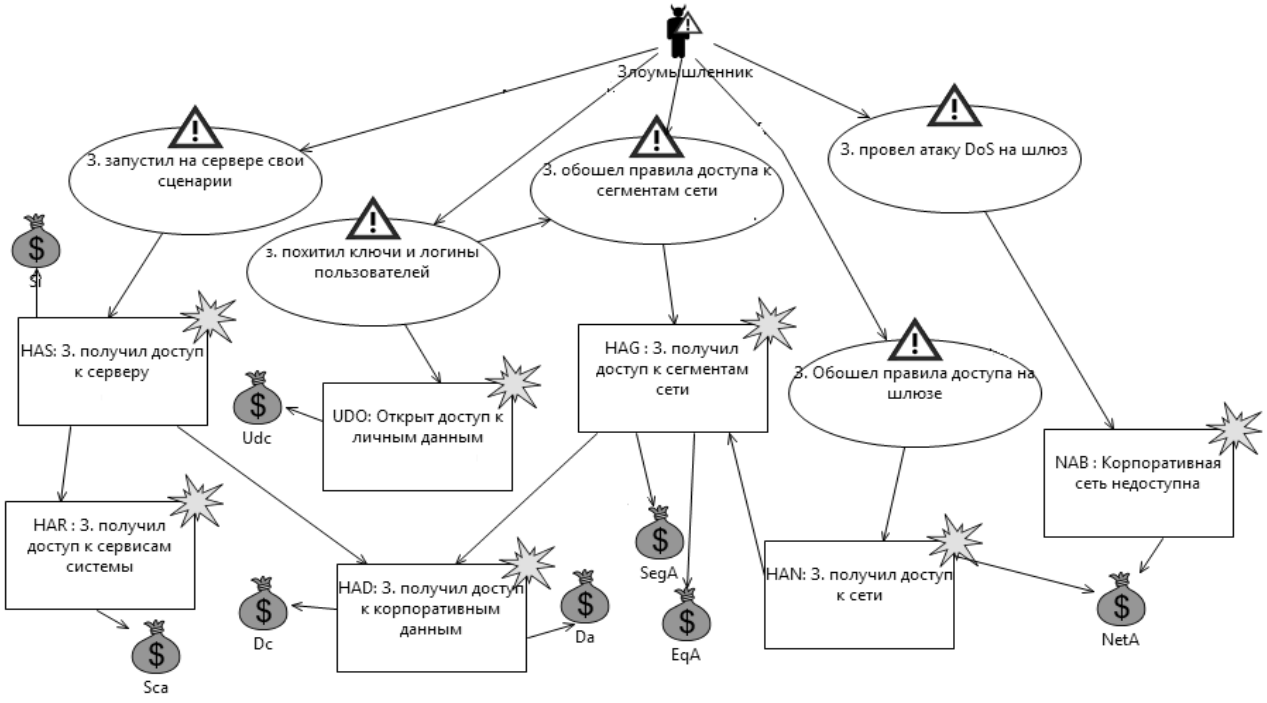


Рисунок 2.1 – Диаграмма угроз «злоумышленник» Coras

Активы: Si = da (Целостность сервера), Da = da (Доступность корпоративных данных), Dc = da (Конфиденциальность корпоративных данных), Sca = da (Доступность сервисов), SegA = da (Доступность сегментов сети), EqA = da (Доступность периферийного и другого оборудования), Uda = da (Доступность пользовательских данных), Udc = da (Конфиденциальность пользовательских данных), NetA – доступность сети.

Все нежелательные инциденты связаны отношением инициализации с угрозами, а также связаны либо отношением следствия с другими инцидентами, либо отношением влияния с конкретными активами.

Данные отношения описаны следующим образом:

Отношения инициализации: $H \xrightarrow{C_{init}(H,HSS)} HSS$ угроза H инициирует сценарий угрозы HSS, при этом переменная $C_{init}(H, HSS)$ описывает вероятность возникновения данного сценария; $H \xrightarrow{C_{init}(H,HSP)} HSP$ угроза H инициирует сценарий угрозы HSP, при этом переменная $C_{init}(H, HSP)$ описывает вероятность возникновения данного сценария; $H \xrightarrow{C_{init}(H,HPA)} HPA$ угроза H инициирует сценарий угрозы HSP, при этом переменная $C_{init}(H, HPA)$ описывает вероятность возникновения данного сценария; $H \xrightarrow{C_{init}(H,HSD)} HSD$ угроза H инициирует сценарий угрозы HSD, при этом переменная $C_{init}(H, HSD)$ описывает вероятность возникновения данного сценария; $H \xrightarrow{C_{init}(H,HPG)} HPG$ угроза H инициирует сценарий угрозы HSD, при этом переменная $C_{init}(H, HPG)$ описывает вероятность возникновения данного сценария.

Отношения наследия, которые связывают сценарии угроз и нежелательные инциденты: $HSS \xrightarrow{C_{Lt}(HSS,HAS)} HAS$ угроза HSS ведет к возникновению нежелательного инцидента HAS, при этом переменная $C_{Lt}(HSS, HAS)$ описывает вероятность возникновения инцидента в результате выполнения сценария; $HSP \xrightarrow{C_{Lt}(HSP,UDO)} UDO$ угроза HSP ведет к возникновению нежелательного инцидента UDO, при этом переменная $C_{Lt}(HSP, UDO)$ описывает вероятность возникновения инцидента в результате выполнения сценария; $HSP \xrightarrow{C_{Lt}(HSP,HPA)} HPA$ угроза HSP ведет к возникновению нежелательного инцидента HPA, при этом переменная $C_{Lt}(HSP, HPA)$ описывает вероятность возникновения инцидента в результате выполнения сценария; $HPA \xrightarrow{C_{Lt}(HPA,HAG)} HAG$угроза HPA ведет к возникновению нежелательного инцидента HAG , при этом переменная $C_{Lt}(HPA, HAG)$ описывает вероятность возникновения инцидента в результате

выполнения сценария; $HPG \xrightarrow{C_{Lt}(HPG,HAN)} HAN$ угроза HPG ведет к возникновению нежелательного инцидента HAN, при этом переменная $C_{Lt}(HPG, HAN)$ описывает вероятность возникновения инцидента в результате выполнения сценария; $HSD \xrightarrow{C_{Lt}(HSD,NAB)} NAB$ угроза HSS ведет к возникновению нежелательного инцидента HAS, при этом переменная $C_{Lt}(HSD, NAB)$ описывает вероятность возникновения инцидента в результате выполнения сценария.

Отношения наследия между нежелательными инцидентами: $HAS \xrightarrow{C_{Lt}(HAS,HAR)} HAR$ нежелательный инцидент HAR вызван нежелательным инцидентом HAS, при этом переменная $C_{Lt}(HAS, HAR)$ описывает степень влияния; $HAS \xrightarrow{C_{Lt}(HAS,HAD)} HAD$ нежелательный инцидент HAD вызван нежелательным инцидентом HAS, при этом переменная $C_{Lt}(HAS, HAD)$ описывает степень влияния; $HAG \xrightarrow{C_{Lt}(HAG,HAD)} HAD$ нежелательный инцидент HAD вызван нежелательным инцидентом HAG, при этом переменная $C_{Lt}(HAG, HAD)$ описывает степень влияния; $HAN \xrightarrow{C_{Lt}(HAN,HAG)} HAG$ нежелательный инцидент HAG вызван нежелательным инцидентом HAN, при этом переменная $C_{Lt}(HAN, HAG)$ описывает степень влияния.

Отношения влияния нежелательных инцидентов на активы системы: $HAS \xrightarrow{C_{imp}(HAS,Si)} Si$ нежелательный инцидент HAS влияет на актив Si, при этом переменная $C_{imp}(HAS, Si)$ описывает степень влияния на оценку актива; $HAR \xrightarrow{C_{imp}(HAR,Sca)} Sca$ нежелательный инцидент HAR влияет на актив Sca, при этом переменная $C_{imp}(HAR, Sca)$ описывает степень влияния на оценку актива; $HAG \xrightarrow{C_{imp}(HAG,SegA)} SegA$ нежелательный инцидент HAG влияет на актив $SegA$, при этом переменная $C_{imp}(HAG, SegA)$ описывает степень влияния на оценку актива; $HAG \xrightarrow{C_{imp}(HAG,EqA)} EqA$ нежелательный инцидент HAG влияет на актив EqA, при этом переменная $C_{imp}(HAG, EqA)$ описывает степень влиянияна оценку актива; $HAN \xrightarrow{C_{imp}(HAN,NetA)} NetA$ нежелательный инцидент HAN влияет на

актив $NetA$, при этом переменная $C_{imp}(HAN, NetA)$ описывает степень влияния на оценку актива; $NAB \xrightarrow{C_{imp}(NAB,NetA)} NetA$ нежелательный инцидент HAB влияет на актив $NetA$, при этом переменная $C_{imp}(HAB, NetA)$ описывает степень влияния на оценку актива; $UDO \xrightarrow{C_{imp}(UDO,Udc)} Udc$ нежелательный инцидент UDO влияет на актив Udc, при этом переменная $C_{imp}(UDO, Udc)$ описывает степень влияния на оценку актива; $HAD \xrightarrow{C_{imp}(HAD,Dc)} Dc$ нежелательный инцидент HAD влияет на актив Dc, при этом переменная $C_{imp}(HAD, Dc)$ описывает степень влияния на оценку актива; $HAD \xrightarrow{C_{imp}(HAD,Da)} Da$ нежелательный инцидент HAD влияет на актив Da, при этом переменная $C_{imp}(HAD, Da)$описывает степень влияния на оценку актива.

Аналогичным образом можно описать любую угрозу, которая способна привести к нарушению безопасности системы. Составленные диаграммы угроз для объектов «вирус», «пользователь», «администратор сети» и «администратор сервисов» представлены в приложении Б. Недостатком такого подхода является угрозоориентированной диаграммы, что дает множество инцидентов от одной угрозы, но, во многих случаях, затрудняет сосредоточиться на защите конкретных активов от наиболее важных инцидентов.

2.1.2 Нечеткий интеграл и нечеткая мера в задачах анализа рисков

Осуществление процесса анализа и оценки риска крайне важно для следующего шага к построению комплексной системы безопасности – обработке риска. Этот шаг предполагает принятие решения о способе реакции на рисковую ситуацию и мерах по ее урегулированию. Таким образом, анализ риска является этапом подготовки данных для принятия решения [43, 69, 78] в задачах многокритериального анализа .

Мера (мера множества) является неотрицательной величиной, которая интуитивно интерпретируется как размер (объем) множества. Формальное определение меры основывается на рассмотрении некоторого произвольного

универсума Z и множества всех его подмножеств 2^Z. Мерой называется функция множества $g: 2^Z \to R$, удовлетворяющая условиям:

1) $A \subseteq 2^Z, g(A) \geq 0$;

2) $g(\emptyset) = 0$;

3) $A, B \subseteq 2^Z, g(A \cup B) = g(A) + g(B) - g(A \cap B)$.

Мера g является мерой вероятности, если R = [0, 1].

Гюстав Шоке предложил применение неаддитивных (нечетких) мер, которые расширяют возможности меры g для моделирования реальных процессов, снимая ограничение аддитивности. В рассматриваемой проблеме нечеткая мера является формализацией связей между критериями. Нечеткой мерой называется функция:

$$\mu: 2^Z \to R$$

которая удовлетворяет условиям:

– условие ограниченности: $\mu(\emptyset) = 0$, $\mu(Z) = 1$;

– монотонность: $A, B \subseteq Z, A \subseteq B, \mu(A) < \mu(B)$;

– непрерывность: $\lim_{m\to\infty} \mu(F_m) = \mu(\lim_{m\to\infty} F_m)$, $F_m \subseteq Z, (m = 1,2, \dots M)$ монотонная последовательность.

Теория нечетких мер и теория нечетких множеств хорошо сочетаются, то есть нечеткий интеграл является удобным инструментом для агрегирования значений функций принадлежности нечетких множеств. Сугено развил идеи Шоке, предложив два вида операторов агрегирования на основе мер [34]. Один из этих видов называется нечетким дискретным интегралом Шоке, а второй – нечетким дискретным интегралом Сугено.

Дискретным интегралом Шоке от функции $h: N \to R^+$ со множеством значений $\{g_1, \dots, g_n\}$) по нечеткой мере μ определяется по формуле:

$$C(\mu, (g_1, \dots, g_n)) = \sum_{i=1}^{n} \left[g_{(i)} - g_{(i-1)}\right] \mu\left(j | h(j) \geq g_{(i)}\right)$$

Интеграл Сугено используется для агрегирования критериев, где на результат агрегирования влияет порядок расположения значений критериев относительно друг друга (порядковые шкалы). Интеграл Шоке [65, 67] применяется для агрегирования, когда на результат влияет величина каждого из критериев, что является важным при решении некоторых проблем выбора.

Для использования интеграла Шоке в многокритериальных задачах [82 – 83, 85] необходимо обеспечить соизмеримость критериев (то есть, в некотором роде свести задачу к случаю $X = Y^n$. На практике идея понятия соизмеримости сводится к тому, что при построении многокритериальной модели следует агрегировать не сами оценки по критериям, а уровни "удовлетворенности" ЛПР, связанные с этими оценками. В литературе по интегралу Шоке на данный момент для преодоления этой проблемы существует два основных подхода. В первом соизмеримость принимается как гипотеза, то есть считается что $X = Y^n$. Во втором подходе в процесс моделирования включается дополнительный шаг - построение соизмеримых функций ценности $f_i: X_i \longrightarrow R, i \in N$ для каждого из критериев, то есть отражение значений всех критериев на единую шкалу.

2.1.3 Нечеткое моделирование в задачах обеспечения информационной безопасности

При решении задач, связанных с обеспечением информационной безопасности, необходимо понимание процессов нарушения состояния системы, которые связанны с проведением атак, совершением ошибок и пр. Для получения сведений об этих процессах, наиболее приемлемым средством является моделирование соответствующих действий [21], связанных с нарушением безопасности. В последнее время получило широкое распространение нечеткое моделирование, так как такой тип моделирования позволят учесть неопределенность [38] как входных данных для моделирования, так и процессов внутри модели. При этом существует широкий набор методов и способов построения нечетких моделей.

Так, в [22] предложен подход к построению нечетких моделей на основе нечетких временных сетей Петри (НСП). При этом выделено несколько классов

таких моделей, основанных на различном наборе нечетких параметров для модели:

– нечеткость задания начальной маркировки. Каждый элемент матрицы начальной маркировки равен значению функции принадлежности наличия числа маркеров в позиции p_i на момент начала запуска НСП;

– нечеткость задания начальной маркировки и срабатывания перехода. По сравнению с предыдущим типом НСП, тут вводится вектор значений функции принадлежности нечеткого срабатывания переходов;

– нечеткость задания начальной маркировки, времен задержки маркеров в позициях и времен срабатывания активных переходов. В дополнение к предыдущему типу вводится вектор временных задержек, где каждый элемент неотрицательная нечеткая величина;

Однако, моделирование процессов нарушения безопасности с использованием нечетких сетей Петри [24] как самостоятельного инструмента имеет ряд недостатков, среди которых отсутствие определения источников событий, неполное описания инцидентов, к которым эти события приводят, сложность и погрешность оценки рисков на основе результатов моделирования.

Чтобы упростить сложные и громоздкие расчеты при моделировании целесообразно воспользоваться специализированными инструментальными средствами, которые позволят автоматизировать весь процесс моделирования или его отдельные этапы [22, 26, 35]. Использование подобных прикладных пакетов позволяет ускорить процесс анализа и обработки данных, полученных в результате моделирования, а также подготовить соответствующие данные для процесса моделирования.

Недостатком использования таких инструментальных средств является платная основа распространения некоторых из них, например среда MATLAB, что может привести к увеличению стоимости процесса моделирования и анализа рисков в целом. Эта проблема может быть разрешена путем поиска свободно распространяемых программ, которые обладают схожим функционалом, или же хотя бы частью необходимых функций. Также, использование сторонних при-

кладных пакетов программ приводит к проблеме совместимости. Результаты работы программы могут храниться в неподходящем формате для программ, используемых на последующих этапах. Поэтому необходимо предусмотреть совместимость форматов или определить преобразование форматов [79 - 80] на промежуточных этапах обработки данных при моделирования и анализа рисков.

2.2 Формирование множества активов информационной системы

Процедура анализа рисков информационной системы начинается с этапа определения множества активов информационной системы (ИС), множества оценок этих активов и множества отношений, описывающих влияние активов друг на друга. Как правило, множество активов формируется путем опроса владельцев активов и других заинтересованных лиц. Активы предприятия могут иметь как абстрактную форму (репутация компании, доверие клиентов и прочее), так и конкретную форму (серверы, сервисы, личные и корпоративные данные, физические устройства и т. п.) Данные элементы множества непрерывно подвергаются влиянию от объектов ИС, а также оказывают влияние на другие элементы. Данное влияние можно представить в виде псевдоиерархической структуры (рисунок 2.2), описывающей зависимости одних активов от других.

На вершине иерархии находится сама ИС или ее транспортная инфраструктура [4, 15]. Именно к ней в первую очередь необходимо получить доступ для дальнейших действий по нанесению вреда. Получив доступ, можно осуществить доступ к трем различным по роду действия активам:

– серверы ИС;

– специализированные сегменты сети;

– конечные устройства легальных пользователей.

Серверы, как правило, обеспечивают сервисы конечных пользователей, как корпоративных, так и внешних. Конечные пользователи хранят личные

данные, которые можно использовать для дальнейшего доступа к периферийным устройствам, серверам и т. п. Специализированные сегменты сети могут представлять собой сети хранения и обработки данных, системы управления производством, кластерные системы. Такие сегменты, которые содержат в себе корпоративные данные, схемы управления процессами и т. д., могут представлять интерес для промышленного шпионажа или кражи.

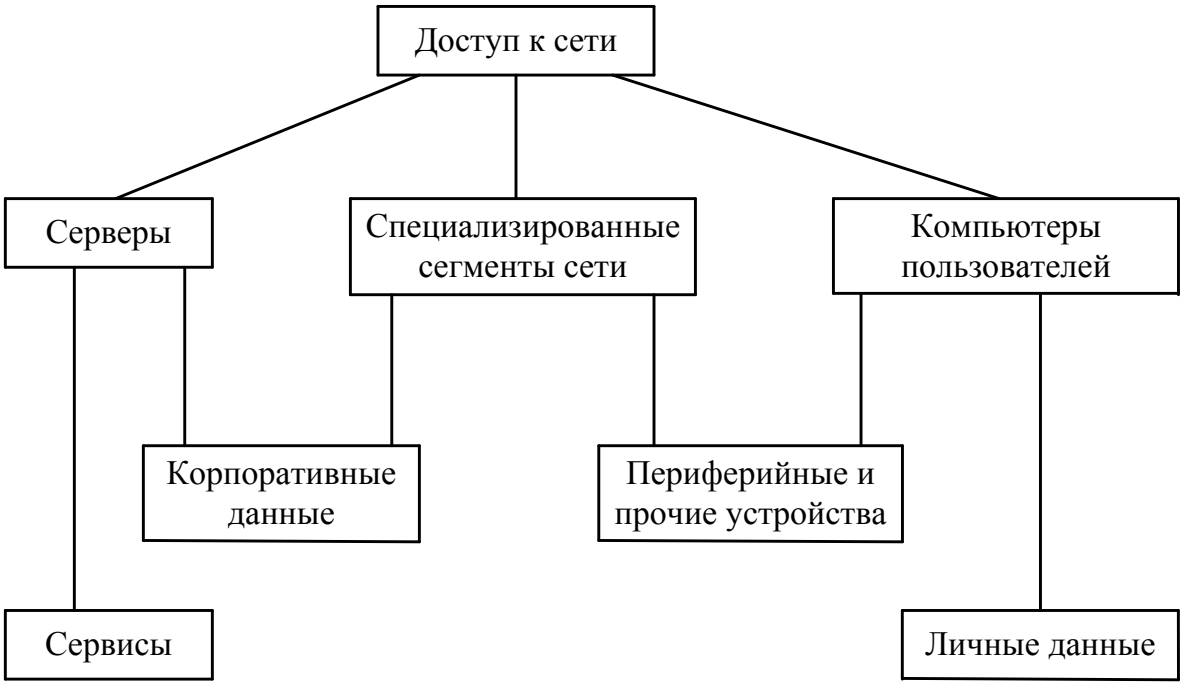


Рисунок 2.2 – Иерархическое взаимодействие активов ИС

Взаимодействие активов выражается в виде отношения вреда, которое характеризует ущерб одного актива вследствие ущерба другому активу [37].

Основными целями атак на активы являются нарушение доступности, целостности либо конфиденциальности. Каждый из представленных активов может быть подвергнут одному и более нарушению. Для построения полноценной диаграммы активов необходимо указать элементы данной диаграммы (активы) с учетом указанных видов нарушений, а также отношения вреда между ними (рисунок 2.3).

При построении диаграммы активов приняты следующие элементы и отношения:

Party = p (название) – Заинтересованное лицо, требующее защиты активов; DirectAsset = da (название, оценка) – прямой актив, подлежащий оценке; IndirectAsset = ia (название, оценка) – непрямой актив, имеющий абстрактную форму; Harm = da→da, da→ia – отношение вреда между активами рассматриваемой системы.

Каждый актив должен иметь свое уникальное имя и иметь оценку важности, которая, на начальном этапе, может быть получена в результате опроса, или быть произвольной. На формирование оценок также влияют отношения между активами, которые также имеют свое значение, выражающее степень тяжести влияния.

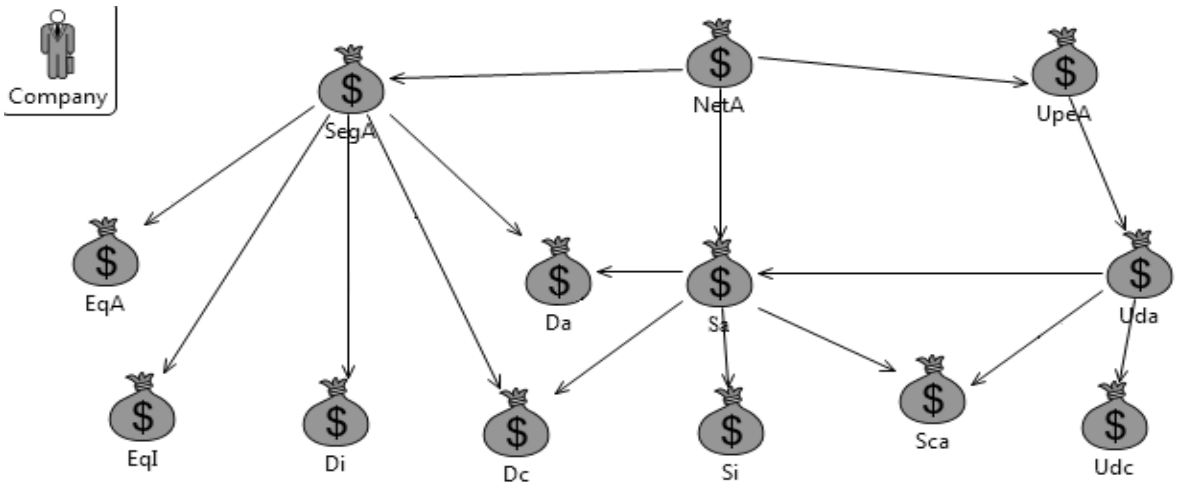


Рисунок 2.3 – Диаграмма активов Coras

Построенная диаграмма имеет следующие элементы: Party = p (Организация); NetA = da (Доступность сети); Sa = da (Доступность сервера); Si = da (Целостность сервера); Da = da (Доступность корпоративных данных); Di = da (Целостность корпоративных данных); Dc = da (Конфиденциальность корпоративных данных); Sca = da (Доступность сервисов); SegA = da (Доступность сегментов сети); EqA = da (Доступность периферийного и другого оборудования); EqI = da (Целостность периферийного и другого оборудования); Uda = da (Доступ-

ность пользовательских данных); Udc = da (Конфиденциальность пользовательских данных).

Как видно из описания элементов, активы системы охватывают все слои ИС, а также описаны с точки зрения доступности, конфиденциальности и целостности. Данную схему, при необходимости, можно обобщить, либо наоборот, еще более детализировать. Отношение вреда устанавливается между парами активов, и описывается следующим образом

$$C_i^{harm} = A_i \xrightarrow{Harm} A.$$

где A_i – актив-источник вреда, A – актив, подверженный ущербу.

Формирование значений отношения вреда представлено далее в данном разделе. Активом источником может быть только физический актив, активом приемником может быть как физический, так и абстрактный.

2.3 Идентификация элементов риска

Предполагается, что на каждый выявленный актив, влияют внешние события, происходящие в информационной системе. Данные события определяют поведение системы в ходе нарушения безопасности и последующий ущерб от реализации данных событий. Для эффективной идентификации данных элементов, целесообразно представить влияние на каждый актив в виде некоторой структуры, которая последовательно описывает все процессы нарушения безопасности и нанесения ущерба каждому активу. Как было показано в пункте 2.1, диаграммами Coras сложно комплексно определить влияние на актив. Однако, данные диаграммы определяют адекватную и удобную терминологию, которая используется в данной работе, в применении к тем структурам, которые разработаны автором. Исходя из этого, в рамках работы было предложено построение псевдоиерархических структур, которые базируются на диаграммах

Coras, но позволяют сосредоточить идентификационный процесс на объекте защиты с установлением причинно-следственных связей для него.

Иерархию элементов структуры угрозы следует строить на основе псевдоиерархической структуры. Данная структура представляет корень, который представляет целевой параметр, вершины – тупиковые и не тупиковые, которые представляют собой параметры, влияющие на поведение системы, и ребра представляют собой взаимосвязь между элементами. Построение данной структуры происходит в несколько этапов.

На *первом* этапе выбирается центральный элемент структуры – актив из выявленного множества $Asset = \{A_1, A_2, \dots, A_n\}$, n – количество выявленных активов.

На *втором* этапе выявляются инциденты, которые могут оказать влияние на выбранный актив. Данные инциденты выбираются либо экспертно, либо определяются статистическими методами (статистика за определенный период, статистика в конкретном регионе и т. п.). В итоге составляется множество инцидентов $UI = \{UI_1, UI_2, \dots, UI_m\}$, m – количество выявленных инцидентов.

На *третьем* этапе определяются сценарии, которые могут привести к инцидентам. В результате выполнения этапа получается множество сценариев $TS = \{TS_1, TS_2, \dots, TS_k\}$, k – количество сценариев, представляющие собой атаки, сбои и ошибки, которые в дальнейшем подлежат моделированию.

На *четвертом* этапе определяются угрозы, которые могут привести к реализации сценариев. Составляется множество угроз $T = \{T_1, T_2, \dots, T_z\}$, z – количество определенных угроз. Данные элементы подлежат дальнейшему разложению на факторы, которые способствуют появлению соответствующей угрозы.

В результате выполнения данных этапов конструируется псевдоиерархическая структура влияния на активы информационной системы, где каждая группа однотипных элементов определяет один уровень структуры. При этом допускаются связи не только между уровнями, но и между элементами одного уровня (рисунок 2.4).

Также, данная структура лишена дублирующихся вершин, которые могут возникнуть в результате взаимодействия нескольких выше стоящих вершин (например, вершина HSP инициирована двумя вершинами H и U), что трудно достижимо в известных методах, где каждая вершина порождает новую вершину.

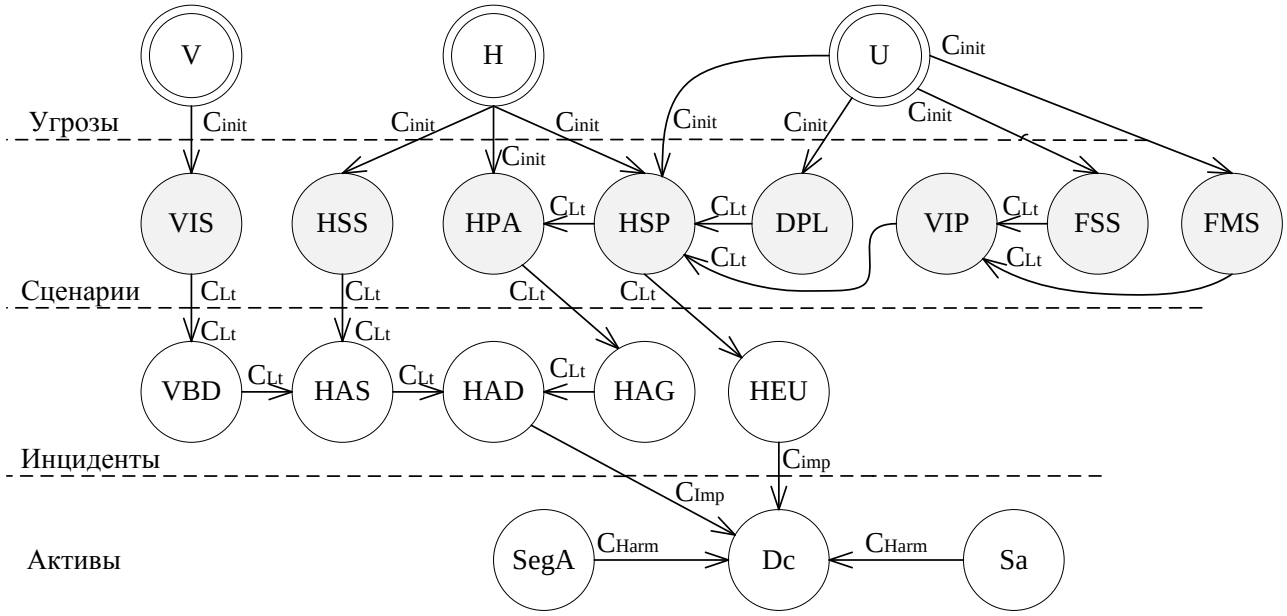


Рисунок 2.4 – Структура влияния на актив «конфиденциальность данных»

Представленная структура демонстрирует влияние на актив «конфиденциальность корпоративных данных». Из представленной структуры можно увидеть, что на актив оказывают влияние 5 инцидентов: VBD – «вирус заблокировал данные», HAS - «хакер получил доступ к серверам», HAD – «хакер получил доступ к данным», HAG – «хакер получил доступ к специфическим сегментам сети», HEU – «хакер вошел в систему с правами пользователя», HAS – «» причем HAD, HEU влияют непосредственно и VBD, HAS, HAG опосредовано.

Такая же ситуация наблюдается и на уровне сценариев. Из выявленного множества сценариев VIS – «вирус инфицировал сервер», HSS – «хакер запустил на сервере свои сценарии», HPA – «хакер обошел правила доступа к сегментам», HSP – «хакер похитил пароли пользователей», непосредственно приводят к инцидентам, а DPL – пользователь дискредитировал пароли или логи-

ны, VIP – вирус инфицирует сервера, FSS – «неправильное пользование поисковыми системами», FMS – неправильное использование почтовыми системами, приводят к срабатыванию других сценариев. Также, на актив оказывают влияние другие активы $SegA$ – «доступность специализированных сегментов» и Sa – «доступность серверов». Другие примеры разработанных структур для выявленных активов представлены в приложении В.

Данный подход к идентификации элементов риска упрощает сопоставление всех инцидентов в системе соответствующим активам, позволяет установить последовательности элементов, которые приводят к ущербу активам. Разбиение структуры на уровни позволяет разделить причины, действия и последствия при реализации нарушения безопасности информационной системы, что позволяет провести раздельную оценку источников нарушения безопасности, моделирование действий при данных нарушениях и оценить события, которые возникли вследствие данных действий.

2.4 Модель взаимодействия активов и инцидентов

Актив представляет собой целевой объект защиты. Предполагается, что защите подлежит как сам актив (сервер, информация и пр.), так и его свойства (доступность, целостность, конфиденциальность, актуальность и др.).

Непосредственно на актив влияют другие активы и инциденты. Соответственно, необходимо разработать математическую модель, которая описывает данное взаимодействие.

Учитывая, что инциденты могут возникать по причине возникновения других инцидентов, а также то, что активы, которые влияют на рассматриваемый актив, тоже подвержены влиянию других элементов риска, структура влияния на актив имеет многоуровневую структуру. В случае, когда на актив влияет только множество инцидентов, описывается одноуровневой структурой (2.1):

$$F(A) = \{C_j^{imp}, P(UI_j)\}_{j=1..m}, \quad (2.1)$$

где $P(UI_j)$ – множество выявленных инцидентов для данного актива, C_j^{imp} – соответствующие им отношения влияния на актив.

Данная модель описывает частные случаи, когда активом выступает обобщенная структура системы (вся система) или же активы верхних уровней структуры, на которые нет влияния других активов.

Однако более частыми ситуациями являются варианты, когда на актив воздействуют другие активы, что предполагает соответствующие коррективы в оценку целевого актива.

Соответственно, необходима модель, которая учитывает не только влияние на актив инцидентов, происходящих в системе, но и активов ущерб которым влияет на ущерб рассматриваемому активу, и модель (2.1) принимает следующий вид:

$$F(A) = \{C_j^{imp}, C_i^{harm}, PA(A_i), P(UI_j)\}_{i=0..n, j=1..m}, \quad (2.2)$$

где $P(UI_j)$ – множество выявленных инцидентов для данного актива, C_j^{imp} – соответствующие им отношения влияния на актив, $PA(A_i)$ – оценка влияющего актива, C_i^{harm} – соответствующее ему отношение вреда.

При этом, если $i = 0$, модель приобретает первоначальный вариант влияния исключительно инцидентов в системе (2.1). В случае $i > 0$, каждый из i-х активов описывается структурами 2.1 или 2.2.

Полученные таким образом модели 2.1 и 2.2 позволяют однозначно сопоставить каждому активу системы соответствующие ему инциденты, возникающие в информационной системе, а также отношения влияния данных инцидентов. Также данные модели позволяют скорректировать оценки активов системы, что позволяет учесть важность актива при оценке соответствующих рисков

для него. Это позволяет в дальнейшем определить соответствующие риски информационной безопасности.

Еще одним частным случаем является определение моделей для непрямых активов. На данные активы не оказывается влияние от элементов риска, кроме прямых (материальных) активов. Соответственно, для данных активов модель (2.2) приобретает вид:

$$F(A) = \{C_i^{harm}, PA(A_i), \}_{i=1..n,},$$

В данной модели элемент A – трактуется как непрямой актив, $PA(A_i)$ – оценка прямого актива, и модель является актуальной при $i > 0$.

Во всех случаях параметр PA характеризует оценку актива, которая является показателем важности актива в рассматриваемой системе [54].

При этом оценка важности актива может состоять из количественной оценки (денежный эквивалент, стоимость восстановления и т. п.) или качественной оценки (важный, критичный и т. п.). После определения активов и отношений между ними, оценивание данных активов и определение силы связей отношений производится с помощью лингвистических переменных. Обозначим через $T(A)$ лингвистическую переменную, которая используется при описании актива A_i. Для этого на множествах значений лингвистических переменных $T(A)$, описывающих систему, определяется множество нечетких термов $T_A = \{T_A^1, T_A^2, \dots, T_A^k\}$ где k – количество термов введенных для описания $T(A)$.

Как правило, оценка активов в известных методиках анализа рисков определяется денежным эквивалентом стоимости данного актива или стоимостью его восстановления. Однако существуют активы, которые либо не имеют денежного эквивалента стоимости, либо этот эквивалент сложно определить. В связи с этим, в данном исследовании, построение терм-множества оценок активов опирается на выявление степени значимости или важности данным акти-

вом. Данный параметр характеризует состояние актива под воздействием на него сторонних факторов

$$T(A) = \{\text{"низкая"}, \text{"умеренная"}, \text{"средняя"}, \text{"высокая"}, \text{"критическая"}\}.$$

Предложенное терм-множество определяет значимость актива от низкой (ущерб активу принесет незначительный ущерб деятельности предприятия, которым можно пренебречь) до критической (ущерб активу может нанести непоправимый вред деятельности предприятия, вплоть до ее остановки). Оценка актива позволяет производить ранжирование активов по степени их важности, что позволяет решить две подзадачи риска:

– провести сортировку выявленных активов по степени их важности;

– установить очередность обработки рисков не только по уровню риска, но и по важности актива.

Данный подход обеспечивает обработку рисков по множеству критериев, которые определяют порядок действий при оценке и обработке рисков.

2.5 Модели инцидентов информационной системы

Так как инцидентом является событие, возникновение которого может нанести ущерб активам системы, необходимо разработать модель, которая позволит описать вероятность возникновения данного инцидента [29, 55]. При этом необходимо учесть неопределенность процессов, которые приводят к конкретному инциденту, а также неопределенность самого инцидента. Такая необходимость обусловлена тем, что само по себе возникновение инцидента в реальных системах не дает гарантии того, что он действительно приведет к ущербу. Чтобы адекватно описать возможность возникновения инцидента необходимо учесть все процессы, которые его инициируют, а также все факторы, которые этому способствуют.

Анализируя построенные при идентификации элементов риска структуры, можно увидеть, что к возникновению инцидентов приводят сценарии и угрозы, с которыми эти сценарии и соответствующие инциденты ассоциированы. Также необходимо учитывать соответствующие отношения между элементами риска. Помимо этого на возникновение каждого инцидента оказывают влияние неявные факторы, такие как уязвимости системы. При этом были выявлены различные варианты взаимодействия указанных элементов на инцидент, в соответствии с которыми были разработаны шесть моделей инцидентов.

Одиночна модель. Простейшая модель описывает возникновение инцидента в результате реализации одного сценария (рисунок 2.5). В соответствии с данной моделью, возникновение инцидента определяется следующими параметрами:

– вероятность угрозы $PT(T)$;

– вероятность осуществления сценария угрозы PX;

– отношение следствия между сценариями угроз и нежелательными инцидентами C^{Lt};

– множество уязвимостей системы $YTS(TS)$ и $YTS(UI)$, которые способствуют реализации сценариев и возникновению инцидентов соответственно;

– вероятность возникновения нежелательного инцидента $P(UI)$.

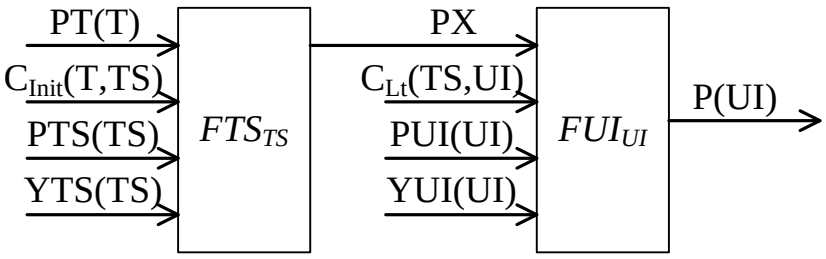


Рисунок 2.5 – Одиночная модель инцидента

Данная модель описывает двухуровневую простую структуру взаимодействия, где блок расчета инцидента представляет собой агрегирование оценки реализации сценария, отношения следствия данного сценария, оценки уязвимо-

стей, которые могут способствовать возникновению данного инцидента и вероятности возникновения самого инцидента. Блок сценария является функцией агрегирования параметров, влияющих на его оценку: вероятность инициирующей его угрозы, отношения инициализации, оценки уязвимостей и вероятности реализации данного сценария. Таким образом, результат $P(UI)$является нечеткой оценкой возможности возникновения данного инцидента

$$P(UI) = F_{UI}(PX, C_{Lt}, PUI(UI), YUI(UI))$$

При этом оценка PX также является функцией агрегирования

$$PX = F_{TS}(PT(T), C_{init}, PTS(TS), YTS(TS))$$

Оператор F представляет собой функцию агрегации входных параметров. В рамках данной работы в качестве такой функции предложено использовать нечеткий интеграл Шоке, который позволяет оценивать выходную величину на основе нечетких мер входных параметров, что позволяет использовать нечетко заданные или не полностью известные параметры.

Последовательная модель. Данная модель описывает случай, когда несколько последовательно выполняемых сценариев приводят к инциденту (рисунок 2.6).

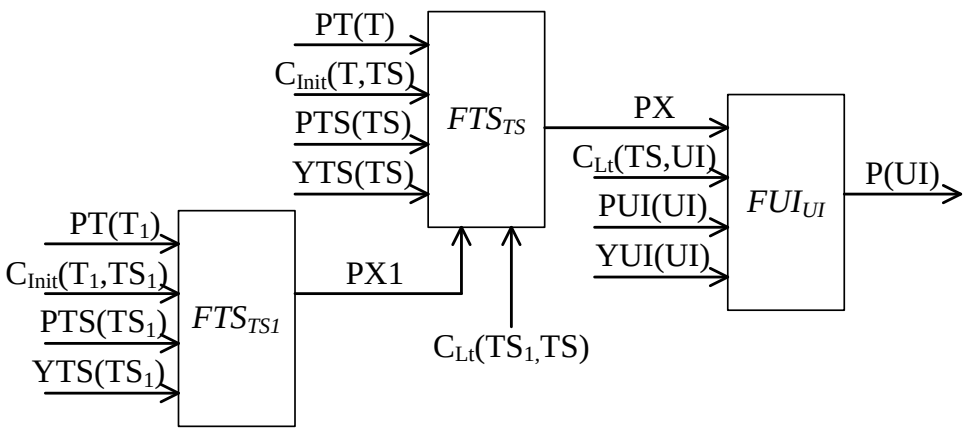


Рисунок 2.6 – Последовательная модель инцидента

Данная модель многоуровневую последовательную структуру, в которой каждый последующий параметр зависит от предыдущего. Таким образом, выходной параметр модели $P(UI)$ определяется последовательно решаемыми нечеткими интегралами для каждого из сценариев

$$P(UI) = F_{UI}\big(PX, C_{Lt}, PUI(UI), YUI(UI)\big),$$
$$PX = F_{TS}(PT(T), C_{init}, PTS(TS), YTS(TS), PX_1),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$PX_i = F_{TS}(PT(T), C_{init}, PTS(TS), YTS(TS), PX_{i+1}).$$

Индекс i определяет количество последовательных интегралов, а $i + 1$ определяет последний уровень вложения модели.

Параллельная модель. Данная модель описывает случай, когда к инциденту приводят независимо исполняемые сценарии (рисунок 2.7).

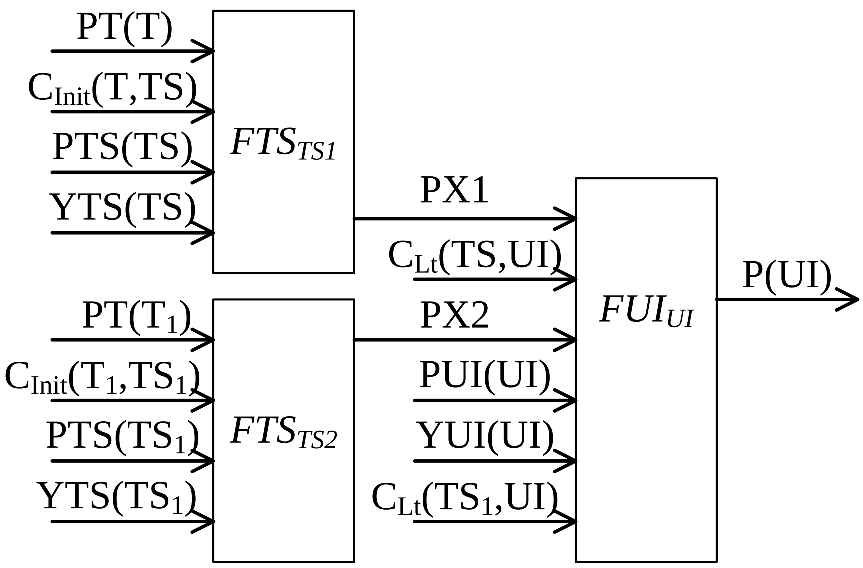


Рисунок 2.7 – Параллельная модель инцидента

Данная модель описывает двухуровневую сложную структуру, которая является расширением одиночной модели. Данная модель позволяет масштаби-

ровать блок расчета оценки возможности возникновения инцидента за счет расширения количества оценок независимых сценариев

$$P(UI) = F_{UI}(C_{Lt}, PUI(UI), YUI(UI), PX_1, \dots, PX_i),$$
$$PX_i = F_{TS}(PT(T), C_{init}, PTS(TS), YTS(TS)),$$

Параллельно-последовательная модель. Данная модель описывает случаи, когда к инциденту приводит выполнение как параллельных, так и последовательных сценариев (рисунок 2.8).

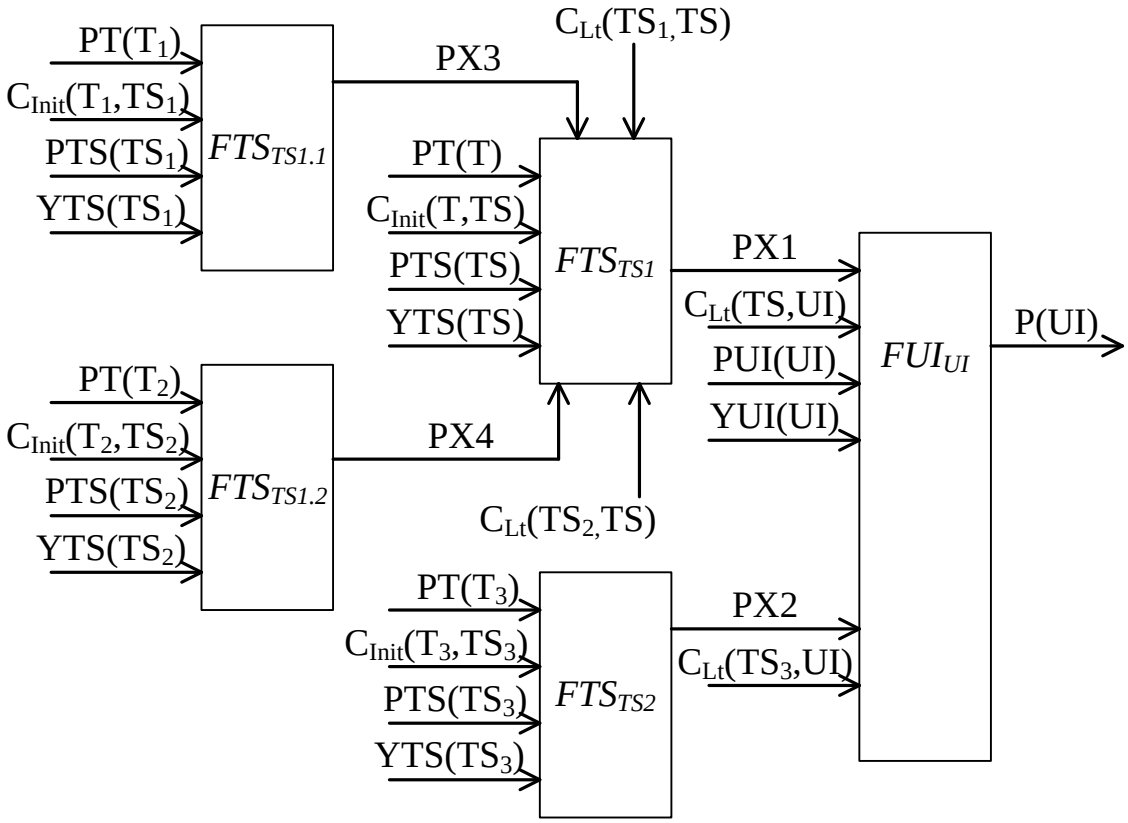


Рисунок 2.8 – Параллельно-последовательная модель

Данная структура описывает многоуровневую сложную структуру, в которой используются разнотипные варианты взаимодействия сценариев. Блок расчета оценки инцидента повторяет структуру параллельной модели, а блоки оценки сценариев комбинируют предыдущие две модели

$$PX_1 = F_{TS}(PT(T), C_{init}, PTS(TS), YTS(TS), PX_{1.1}),$$

……

$$PX_1 = F_{TS}\left(PT(T), C_{init}, PTS(TS), YTS(TS), PX_{1.j}\right),$$

……

$$PX_i = F_{TS}\left(PT(T), C_{init}, PTS(TS), YTS(TS), PX_{i.j}\right),$$

Одиночная модель инцидент-инцидент. Модель, которая описывает случаи, в которых инцидент возникает вследствие возникновения другого инцидента (рисунок 2.9).

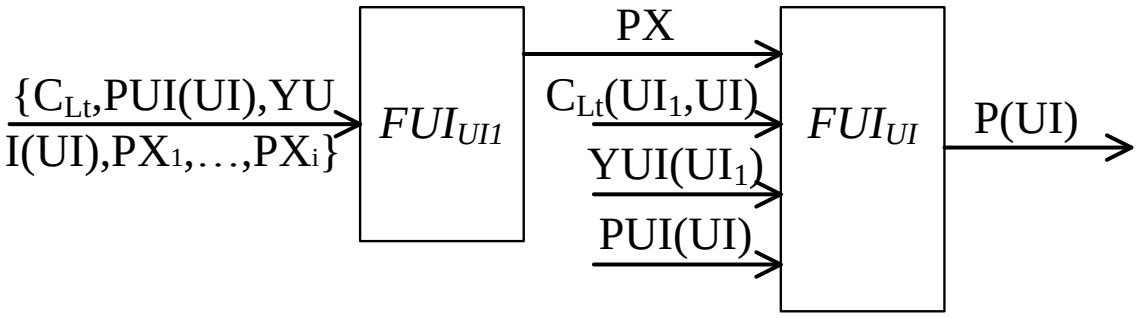


Рисунок 2.9 – Одиночная модель инцидент-инцидент

Данная модель описывает взаимодействие исключительно между инцидентами. В данном примере описано взаимодействие между двумя инцидентами

$$P(UI) = F_{UI}(C_{Lt}, PUI(UI), YUI(UI), PX),$$

При этом допускается масштабирование модели аналогично предыдущим моделям, если на возникновение инцидента оказывают влияние несколько инцидентов.

Смешанная модель. Данная модель объединяет все модели связанные со сценариями и инцидентами (рисунок 2.10).

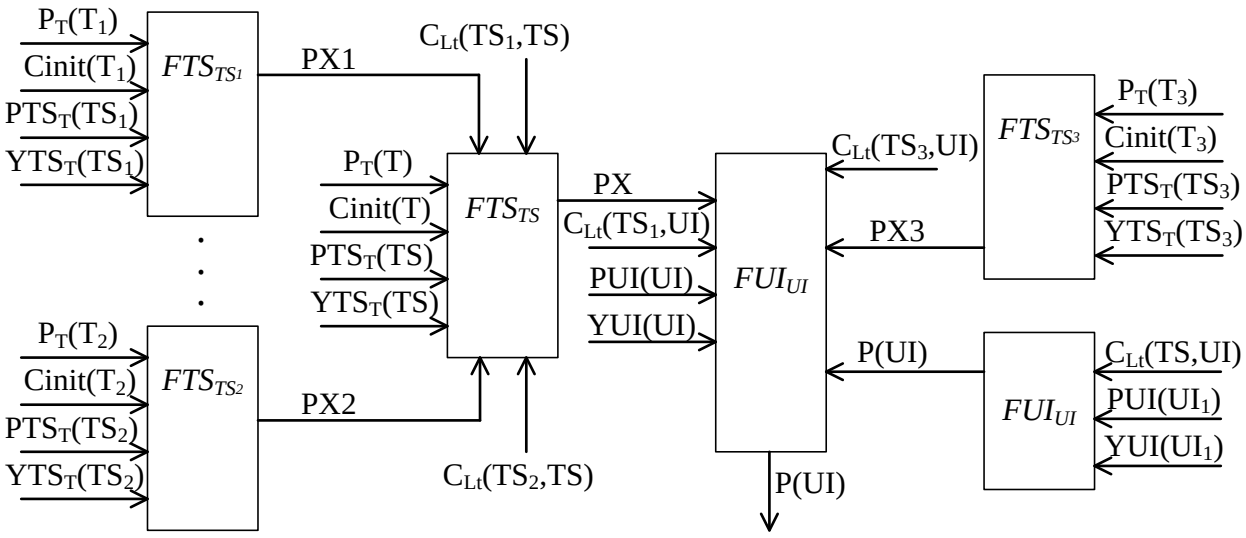


Рисунок 2.10 – Смешанная модель инцидентов

Данная модель объединяет в себе все рассмотренные модели, когда на возникновение инцидента влияют как сценарии, так и другие инциденты.

Блоки вычисления сценариев являются идентичными блокам вычисления в параллельно-последовательной модели, а блок расчета оценки инцидента определяется идентично параллельной модели, с единственным отличием, что оценки PX_i определяют не только оценками сценариев, но и оценками инцидентов.

2.6 Определение отношений между элементами риска

Отношения между элементами характеризуют степень воздействия одного элемента на другой, и имеют индивидуальных характер описания для каждого типа элемента.

Как видно из структуры, построенной в результате идентификации элементов риска, между ними возможны четыре вида отношений – отношение инициализации, следствия, влияния и вреда [37, 55]. В таблице 2.1 можно увидеть, между какими элементами возможны соответствующие типы отношений.

Степень воздействия каждого типа отношения определяется как типом элемента (актив, риск, угроза, сценарий, инцидент), так и индивидуальными свойствами самого элемента.

Как видно из таблицы 2.1, возможны различные способы определения значения отношений. Вероятностные или бальные оценки определяются экспертами, и основываются на экспертных знаниях или статистическом анализе предметной области (основываясь на личном опыте, статистике за промежуток времени или в конкретном регионе) и являются количественными оценками. Лингвистические значения отношений [81] определяют качественную оценку параметра, что позволяет определять данные параметры не только специалистам, но и другим участникам анализа рисков нетехнического профиля.

Таблица 2.1 – Варианты отношений между элементами риска

Тип отношения	Элементы	Имя переменной	Тип значений
Вред	Актив-Актив	C_{harm}	Лингвистическая
Инициализация	Угроза-Сценарий	C_{init}	Лингвистическая Вероятность
Следствие	Сценарий-Сценарий Сценарий-Инцидент Инцидент-Инцидент	C_{Lt}	Лингвистическая Вероятность
Влияние	Инцидент-Актив Риск-Актив	C_{imp}	Лингвистическая Бальная шкала

Отношение инициализации описывает возможность того, что угроза может способствовать реализации определенных сценариев. Данное отношение описывает классическую вероятностную характеристику события в системе, или может быть выражено лингвистически

$$T(init) = \{\text{"вряд ли"}, \text{"вероятно"}, \text{"}скорее\ всего\text{"}\},$$

Фактически данные параметры определяют, в какой мере возможна реализация каждого сценария, если в системе обнаружена связанная с ним угроза. При этом формальное описание данных термов должно иметь соответствие в терминах естественного или математического языков:

– «вряд ли» – вероятность инициализации меньше 0,3 или равна 1-4 баллам;

– «вероятно» – вероятность инициализации 0,4-0,6 или равна 5-7 баллов;

– «скорее всего» – вероятность инициализации больше 0,7 или равна 8-12 баллам;

Отношение следствия описывает возможность возникновения некоторого события в результате выполнения другого события. Также как и отношение инициализации, данный тип отношения может быть оценен вероятностной величиной или лингвистической переменной

$$T(Leads\ to) = \{\text{"}возможно\text{"}, \text{"}скорее\ всего\text{"}, \text{"}обязательно\text{"}\},$$

Данные термы конструируются таким образом, чтобы качественно описывать причинно-следственные связи между сценариями и инцидентами, и наступление одного события в той или иной мере приведет к наступлению другого события. Также данные термы должны иметь некоторое исчислимое соответствие для дальнейшей обработки, аналогичное отношению инициализации.

Отношение влияния характеризует степень ущерба для актива, под воздействием некоторого инцидента или инцидентов. Лингвистические термы данной переменной зависят от типа актива и инцидента. Данные термы могут описывать юридические, экономические, технические или другие последствия нарушения свойств актива. Например, нарушение доступности платных серви-

сов хостинга могут быть описаны для экономических последствий следующим образом

$$T(Impact) = \{"незначительный", "умеренный", "серьезный", "критический"\},$$

Причем сопоставление с реальными последствиями может быть следующим:

– «незначительные» – простой системы менее 4 часов, без штрафных санкций;

– «умеренные» – простой системы от 4 до 6 часов, штрафные санкции небольшие;

– «серьезные» – простой системы от 6 до 8 часов, штрафные санкции большие;

– «критические» – простой системы более 8 часов, штрафные санкции могут привести к закрытию хостинга.

Отношение вреда характеризует взаимодействие между активами и описывает последствия для актива от ущерба другому активу

$$T(Harm) = \{"малый", "заметный", "крайний"\},$$

что может трактоваться, продолжая предыдущий пример, следующим образом:

– если ущерб доступности сервисов «незначительные», то ущерб репутации «малый»;

– если ущерб доступности сервисов «умеренные» или «серьезные», то ущерб репутации «заметный»;

– если ущерб доступности сервисов «критические», то ущерб репутации «крайний».

Таким образом, формирование значений для отношений, позволяет качественно или количественно описать взаимодействие объектов и событий в системе во время нарушения информационной безопасности. Это позволяет математически описать переходы между вершинами идентификационной структуры или, говоря о реальных объектах, определить возможности последствий от возникающих в системе событий.

2.7 Выводы

В данном разделе проанализированы наиболее популярные инструментальные и математические средства, которые используются при анализе данных, и могут быть использованы в ходе осуществления анализа рисков. Определены элементы риска, которые непосредственно участвуют в формировании рисков информационной безопасности. При этом:

– показан процесс выявления и оценки активов, которые подлежат защите. Данный процесс характеризуется тесным взаимодействием всех заинтересованных лиц, которые имеют отношение к информационной системе;

– проведена идентификация элементов рисков информационной системы. Предложен способ идентификации, который предусматривает построение структуры, целевым объектом которой является непосредственно объект защиты (актив и его свойства) и устанавливаются связи этого объекта с другими элементами риска;

– разработаны модели описания взаимодействия активов и инцидентов, которые позволяют строить многоуровневые структуры влияния на рассматриваемый актив;

– предложена модификация оценки активов информационной системы, которая позволяет проводить ранжирование важности активов информационной системы на основе термов лингвистической переменной. Данный подход позволяет участвовать в процессе оценки не только специалистам информаци-

онной безопасности, но и другим лицам, не имеющим специальных навыков в предметной области;

– предложено семейство моделей, которые описывают возникающие в системе инциденты безопасности. Это позволило моделировать сложные структуры взаимодействия сценариев и инцидентов;

– предложен способ оценки отношений между элементами риска, который основывается на лингвистических, вероятностных или бальных оценках и позволяет определять степень воздействия одного элемента риска на другой, а также оценивать ущерб активам информационной систем, что необходимо при идентификации и оценке соответствующих рисков безопасности.

РАЗДЕЛ 3
МОДЕЛИРОВАНИЕ СЦЕНАРИЕВ НАРУШЕНИЯ БЕЗОПАСНОСТИ. ОЦЕНКА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Как было показано в предыдущей главе, основными элементами, формирования рисков для активов информационной безопасности являются инциденты, возникающие в информационной системе, и степень ущерба от данных инцидентов. При этом степень ущерба задается с использованием отношения влияния, а оценку инцидента [29] необходимо рассчитать на основе множества параметров. Для этого необходимо оценить сценарии, которые приводят к возникновению инцидентов и угрозы, которые приводят к данным сценариям.

Сценарии описывают процессы в информационной системе, которые осуществляются под воздействием некоторой угрозы или нескольких угроз, и определяют последовательность действий, которые приводят к инцидентам безопасности.

При этом было выявлено четыре типа сценариев, которые характеризуют сценарии с точки зрения IT-угроз:

– атаки. Данный тип сценариев описывает действия злоумышленников, вирусов, инсайдеров и т.д. Характерной особенностью данных сценариев является описание последовательности действий, которые способствуют реализации сценария;

– ошибки. Данный тип сценариев описывает неправильные действия или бездействие пользователей системы, связанные с низкой компьютерной грамотностью пользователей, квалификацией администраторов и т. п. Характерной особенностью данных сценариев является оценка на основе показателей возможности возникновения конкретной ошибки;

– сбои. Данный тип сценариев описывает системные сбои, которые возникают под воздействием внутренних или внешних факторов. Характерной особенностью данных сценариев является нечеткая оценка ожидания сбоя;

– отказы. Отличаются от сбоев длительным бездействием объекта или его полным выходом из строя.

Известные способы моделирования компьютерных атак опираются на вероятностные характеристики процессов осуществления нарушений [71]. Однако, как было показано в первом разделе, данный подход полностью не оправдывает себя, в связи с априорным свойством данных оценок. Также, вероятностные подходы не позволяют оценивать процессы в условиях ограниченных знаний о процессе или объекте. Все это не дает возможности эффективно оценивать сценарии, которые осуществляются в условиях неопределенности и постоянной угрозы.

В связи с этим было решено использовать в качестве математического аппарата моделирования элементы нечеткой логики, а именно нечеткие числа в качестве характеристик процессов атак.

3.1 Нечеткие параметры сценариев нарушения безопасности

При описании нечетких параметров необходимо описать нечеткие значения, которые они принимают. Чтобы избежать многозначности трактовки семантических значений одного и того же параметра в различных ситуациях, построим полные ортогональные семантические пространства, которые будут служить областями нечетких значений каждого из параметров вне зависимости от рассматриваемой системы [66, 73, 86, 88, 90, 91].

Для построения полного ортогонального семантического пространства (ПОСП) некоторого нечеткого параметра $\tilde{p}_i$ определим множества нечетких значений $D_i = \{p_i^k\}_{k=1..K_i}$, где K_i – количество нечетких значений, принимаемых i-м параметром, в виде нечетких чисел с треугольной функцией принадлежно-

сти μ_i^k, которая положительно определена на некотором интервале $\left(p_{ib}^k, p_{ie}^k\right)$, где $p_{ib}^k, p_{ie}^k \in D$ - значения начала и конца интервала соответственно, а D_i – базовое множество нечетких значений параметра p_i. Для того чтобы построенные множества D_i являлись ПОСП, необходимо, чтобы они удовлетворяли следующим аксиомам [4].

Предположим, что параметру $\widetilde{p_i}$ дан набор чисел $\{a_{ij}\}_{j=0}^n$, определяемый соотношениями

$$a_{ij} = a_i + \frac{(b_i - a_i)}{n_i} j, j = 0 \dots n_i, \tag{3.1}$$

где $D_i = [a_i, b_i]$–некоторый заданный сегмент на действительной оси, а n_i – некоторое целое число

Используя данный набор чисел из (3.1) можно построить пост ортогональное семантическое пространство $\Xi_A(i)$, термы которого задаются формулой

$$A_{ij} = \begin{cases} (a_i, a_i, a_{i1}), j = 0 \\ \left(a_{ij-1}, a_{ij}, a_{ij+1}\right), 1 \le i < n_i \\ \left(a_{in_i-1}, a_{in_i}, a_{in_i+1}\right), i = n_i \end{cases} \tag{3.2}$$

В данном выражении $A = (a_{min}, a, a_{max})$ обозначается треугольное нечеткое число, функция принадлежности $\mu_A(x)$ которого определяется формулой

$$\mu_A(x) = \begin{cases} 0, x < a_{min}, x > a_{max}, \\ \frac{x - a_{min}}{a - a_{min}}, a_{min} \le x \le a, \\ 1, x = a \\ \frac{a_{max} - x}{a_{max} - a}, a \le x \le a_{max} \end{cases} \tag{3.3}$$

В общем случае, нечеткое треугольное число $S_i = (s_{i,min}, s_i, s_{i,max})$, которое описывает значение параметра $\widetilde{p_i}$, не будет совпадать ни с одним из нечетких значений из ПОСП Ξ_A. Для определения соответствия полученного значения какому то из нечетких значений из ПОСП Ξ_A, можно использовать разные метрические отношения.

Зададим соответствующее метрическое отношение формулой

$$S_i(\Xi) = arg\ \min_j f_d(A_{ij}, S_i) \tag{3.4}$$

где $f_d(A_{ij}, S_i) = |s_i - a_{ij}|$

Тогда справедливо следующее утверждение.

Теорема 1. Пусть дано ПОСП $\Xi_A(i)$определенное соотношениями (3.2). А соответствие нечеткого треугольного числа $S_i = (s_{i,min}, s_i, s_{i,max})$, нечеткому значению A_{ij} из ПОСП $\Xi_A(i)$, устанавливается с помощью соотношений (3.3)-(3.4). Тогда нечеткое число $S_i(\Xi)$ определяется с помощью соотношения

$$S_i(\Xi) = \begin{cases} A_{i,\left[\frac{s_i - a_i}{b_i - a_i} n_i\right]+1}, \dfrac{s_i - a_i}{b_i - a_i} n_i - \left[\dfrac{s_i - a_i}{b_i - a_i} n_i\right] > 0.5 \\ A_{i,\left[\frac{s_i - a_i}{b_i - a_i} n_i\right]}, \dfrac{s_i - a_i}{b_i - a_i} n_i - \left[\dfrac{s_i - a_i}{b_i - a_i} n_i\right] \leq 0.5 \end{cases}$$

Применяя полученный результат можно описать несколько вспомогательных моделей.

Обозначим через $\tilde{x} = \{x_b, x, x_e\}$, $\tilde{y} = \{y_b, y, y_e\}$ и $\tilde{z} = \{z_b, z, z_e\}$ некоторые нечеткие числа с функциями принадлежности вида (3). Тогда согласно [5] можно написать

$$\tilde{z} = \tilde{x} @ \tilde{y} = \bigcup_\alpha z_\alpha = \bigcup_\alpha x_\alpha @ y_\alpha \tag{3.5}$$

где $x_\alpha, y_\alpha, z_\alpha$ – α-уровни нечетких значений $\tilde{x}, \tilde{y}, \tilde{z}$ соответственно; а символом @ обозначается один из символов$\{+, -, *, /\}$. При этом справедливы следующие соотношения

$$x_\alpha + y_\alpha = \{x_{\alpha b} + y_{\alpha b}, x_{\alpha e} + y_{\alpha e}\}$$
$$x_\alpha - y_\alpha = \{x_{\alpha b} - y_{\alpha b}, x_{\alpha e} - y_{\alpha e}\}$$
$$x_\alpha * y_\alpha = \begin{Bmatrix} \min(x_{\alpha b} * y_{\alpha b}, x_{\alpha b} * y_{\alpha e}, x_{\alpha e} * y_{\alpha b}, x_{\alpha e} * y_{\alpha e}) \\ \max(x_{\alpha b} * y_{\alpha b}, x_{\alpha b} * y_{\alpha e}, x_{\alpha e} * y_{\alpha b}, x_{\alpha e} * y_{\alpha e}) \end{Bmatrix}$$
$$\frac{x_\alpha}{y_\alpha} = x_\alpha * \frac{1}{y_\alpha} = \left\{ min\left(\frac{x_{\alpha b}}{y_{\alpha b}}, \frac{x_{\alpha e}}{y_{\alpha b}}, \frac{x_{\alpha b}}{y_{\alpha e}}, \frac{x_{\alpha e}}{y_{\alpha e}}\right) max\left(\frac{x_{\alpha b}}{y_{\alpha b}}, \frac{x_{\alpha e}}{y_{\alpha b}}, \frac{x_{\alpha b}}{y_{\alpha e}}, \frac{x_{\alpha e}}{y_{\alpha e}}\right) \right\} \quad (3.6)$$

Учитывая треугольность функций принадлежности, можно (3.6) с учетом (3.5) переписать в следующем виде

$$\tilde{z} = \tilde{x} + \tilde{y} = \{x_b + y_b, x + y, x_e + y_e\}$$
$$\tilde{z} = \tilde{x} - \tilde{y} = \{x_b - y_b, x - y, x_e - y_e\}$$
$$\tilde{z} = \tilde{x} * \tilde{y} = \{x_b * y_b, x * y, x_e * y_e\}$$
$$\tilde{z} = \tilde{x}/\tilde{y} = \{x_b/y_b, x/y, x_e/y_e\}$$

Модель 1. Пусть заданы множества входных параметров $X = \{x_i\}$, $A = \{a_i\}$, $X \cap A = \emptyset$ и выходной параметр y, причем, каждый параметр является нечетким и его значение определяется функцией принадлежности типа (3.3). Тогда каждый параметр будет определяется тремя значениями

$$\mathrm{x} = \{\mathrm{x_{ib}}, \mathrm{x_i}, \mathrm{x_{ie}}\}$$
$$\mathrm{a} = \{\mathrm{a_{ib}}, \mathrm{a_i}, \mathrm{a_{ie}}\}$$
$$\mathrm{y} = \{\mathrm{y_b}, \mathrm{y}, \mathrm{y_e}\}$$

Рассмотрим случай, когда отображение имеет следующий вид

$$y = \sum_i a_i x_i$$

Применяя для решения соотношения (3.6) формулы (3.3-3.5) получим нечеткое значение параметра $\boldsymbol{y}$, которое определяется следующим выражением

$$y = arg \min_{k=1..K_y} f_d(y^k, y')$$

Здесь y'нечеткое треугольное число определяемое соотношениями

$$y' = (\sum_i a_{ib} x_{ib}, \sum_i a_i x_i, \sum_i a_{ie} x_{ie})$$

Модель 2. Пусть заданы множества входных параметров $\widetilde{X} = \{\widetilde{x}_i\}$, $\widetilde{A} = \{\widetilde{a}_i\}$, $\widetilde{X} \cap \widetilde{A} = \varnothing$ и выходной параметр $\tilde{y}$, причем, каждый параметр является нечетким и его значение определяется функцией принадлежности типа (3). Тогда каждый параметр будет определяется четырьмя значениями

$$\widetilde{x_i} = \{x_{ib}, x_i, x_{ie}\},$$
$$\widetilde{a_i} = \{a_{ib}, a_i, a_{ie}\},$$
$$\widetilde{y_i} = \{y_{ib}, y_i, y_{ie}\}.$$

Рассмотрим случай, когда выходное отображение имеет следующий вид

$$y = \frac{1}{\sum_i a_i} \sum_i a_i x_i$$

Применяя для данного соотношения формулы (3.3-3.4) получим нечеткое значение параметра $\tilde{y}$, которое определяется следующим выражением

$$y = arg \min_{k=1..k_y} f_d\,(y_i^k, y')$$

Здесь y′нечеткое треугольное число определяемое соотношениями

$$y' = (z_2, z_3, z_1)$$

где $z_1 = \frac{1}{\sum_i a_{ib}} \sum_i a_{ie} x_{ie}$, $z_2 = \frac{1}{\sum_i a_{ie}} \sum_i a_{ib} x_{ib}$, $z_3 = \frac{1}{\sum_i a_i} \sum_i a_i x_i$

Модель 3. Пусть задано множество входных параметров $\{\mathrm{fx}_1, \mathrm{fx}_2\}$, и выходной параметр fy, причем, каждый параметр является нечетким и его значение определяется функцией принадлежности типа (3.3). Тогда каждый параметр будет определяться тремя значениями

$$fx_i = \{x_{ib}, x_i, x_{ie}\}, i = 1,2,$$
$$fy = \{y_b, y, y_e\}.$$

Рассмотрим случай, когда выходное отображение имеет следующий вид:

$$fy = \frac{fx_1 fx_1 + fx_1 fx_2 + fx_2 fx_2}{fx_1 + fx_2}$$

Применяя для соотношения (*) формулы (-) получим нечеткое значение параметра *fy*, которое определяется следующим выражением:

$$y = arg\, min_{k=1..k_y} f_d\,(y_i^k, y_i').$$

Здесь y' нечеткое треугольное число определяемое соотношениями

$$y' = (z_2, z_3, z_1)$$

где, $z_1 = (x_{1b}x_{1b} + x_{1b}x_{2b} + x_{2b}x_{2b})/(x_{1e} + x_{2e})$,

$z_2 = (x_1x_1 + x_1x_2 + x_2x_2)/(x_1 + x_2)$,

$z_2 = (x_{1e}x_{1e} + x_{1e}x_{2e} + x_{2e}x_{2e})/(x_{1b} + x_{2b})$.

3.2 Моделирование сценариев угроз

Для определения оценок сценариев, необходимо осуществить их моделирование с учетом нечетких характеристик функционирования [32, 68, 72, 74]. Так как атаки на систему представляют собой последовательность действий, необходимо определить аппарат, который позволит описывать эти этапы, а также использовать нечеткие параметры при описании атаки. Для этих целей было предложено использовать нечеткие временные сети Петри, что позволяет нечетко описать временные характеристики атак и оценить вероятность их реализации.

В ходе построения структур атак можно увидеть, что этапы реализации атаки взаимодействуют двумя способами – параллельно и последовательно. В классических сетях Петри [22, 32] данное взаимодействие описывается линейной суммой для последовательных этапов, и сложной структурой для параллельных этапов. Для описания данных типов взаимодействий необходимо воспользоваться соответствующими операциями для нечетких чисел. В соответствии с этим используется три типа операций.

Первый тип операций позволяет получать значения линейных сумм параметров, которые характерны для последовательных этапов реализации сценария

$$\tau_k = \sum \tau_{ij} = \{\sum \tau_{ij}, \sum \alpha_{ij}, \sum \beta_{ij}\},$$

где τ_{ij} – значения нечеткого числа,

α_{ij} – левая граница числа,

β_{ij} – правая граница числа

Второй тип операций позволяет вычислять произведения двух параметров

$$\tau_k = \tau_1 * \tau_2 = \{\tau_1 * \tau_2, \tau_1\alpha_2 + \tau_2\alpha_1, \tau_1\beta_2 + \tau_2\beta_1\}.$$

Типовой задачей в моделях сценариев является умножение только двух параметров и другие случаи не рассматриваются в данном контексте.

Третий тип операций определяет деление нечетких чисел:

$$\tau_k = \frac{\tau_1}{\tau_2} = \left\{\frac{\tau_1}{\tau_2}, (\tau_1\alpha_2 + \tau_2\alpha_1)/\tau_2^2, (\tau_1\beta_2 + \tau_2\beta_1)/\tau_2^2\right\}.$$

Обозначив фрагменты $\tau_1\alpha_2 + \tau_2\alpha_1$ и $\tau_1\beta_2 + \tau_2\beta_1$ как α_{21} та β_{21} соответственно, выражения произведения и деления можно переписать

$$\tau_k = \tau_1 * \tau_2 = \{\tau_1 * \tau_2, \alpha_{21}, \beta_{21}\},$$

$$\tau_k = \frac{\tau_1}{\tau_2} = \left\{\frac{\tau_1}{\tau_2}, \alpha_{21}/\tau_2^2, \beta_{21}/\tau_2^2\right\}.$$

Использование всех трех типов операций позволяет определять параметры параллельных этапов сценариев, где используются все указанные выше операции.

Сеть Петри строится для определения соответствующих этапов атаки [53, 59, 60] и представляется в графическом виде (рисунок 3.1). Классические сети Петри позволяют на основе матриц срабатывания переходов и дифференциальных уравнений определить время перехода по сети и определить вероятность осуществления атаки, описываемой данной сетью [23].

Каждое состояние S_i и переход t_j определяют соответствующие временные параметры τ_{ij}, которые характеризуют время выполнения соответствующего этапа.

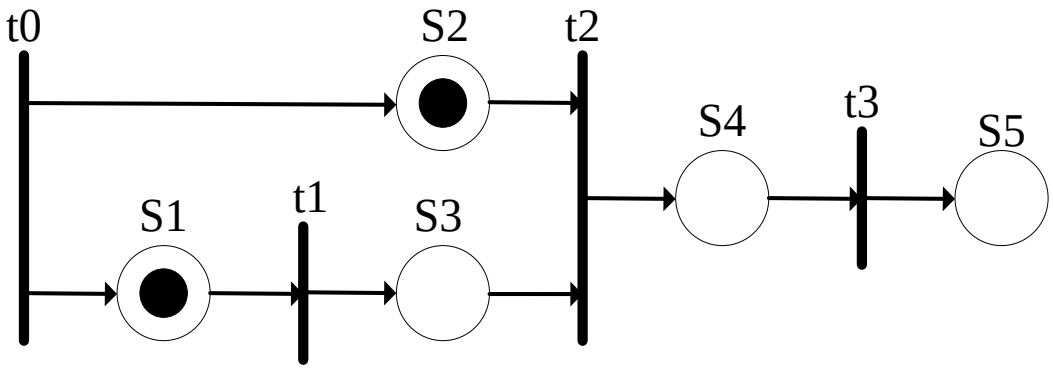


Рисунок 3.1 – Модель сценария DoS атаки (HSD)

Например для указанной модели атаки итоговое выражение для вычисления общего времени прохода по сети следующее:

$$\tau_1 = \tau_{11} + \tau_{32}$$

$$\tau_2 = \frac{\tau_1^2 + \tau_1\tau_{22} + \tau_{22}^2}{\tau_1 + \tau_{22}}$$

$$\tau = \tau_2 + \tau_{43}$$

В ходе составления выражения целесообразно его декомпозировать на составные части, которые описывают параллельное или последовательное взаимодействие этапов атаки.

Однако, при использовании классических сетей, параметры τ_{ij} задаются точными значениями или усредняются, что снижает точность итогового результата модели. К тому же, не всегда возможно определить точные параметры для модели, в силу неопределенности некоторых этапов процесса атаки. Поэтому, в диссертационной работе предложено использовать приблизительные оценки параметров, которые характеризуют этапы осуществления атаки.

$$\tau_{ij}(HSD) = \left[a_{ij}(HSD), b_{ij}(HSD)\right],$$

где a_{ij}, b_{ij} – левая и правая границы заданного диапазона

В соответствии с этим, вычисление времени прохождения по сети описывается следующим выражением

$$\tau_1(HSD) = \tau_{11}(HSD) + \tau_{32}(HSD)$$

$$\tau_1(HSD) = \frac{\tau_1^2(HSD) + \tau_1(HSD)\tau_{22}(HSD) + \tau_{22}^2(HSD)}{\tau_1(HSD) + \tau_{22}(HSD)}$$

$$\tau(HSD) = \tau_2(HSD) + \tau_{43}(HSD)$$

где $\tau_{ij}(HSD)$ - одно из значений диапазона $\left[a_{ij}(HSD), b_{ij}(HSD)\right]$

На основе входных данных генерируется система нечеткого логического вывода. Функции принадлежности этих данных определяются таким образом, чтобы термы переменных равномерно распределялись в середине диапазона этих данных. При этом генерируется все возможное множество правил вывода. Для обучения системы вывода используются результаты имитационного моделирования соответствующей атаки. Определяется количество точек дискретизации функции принадлежности при осуществлении нечеткого логического вывода.

В результате осуществления данных операций определяется матрица выходных значений, правила для нечеткой базы знаний в соответствии с входными переменными, и другие параметры нечеткого вывода.

Получив множество выходных значений, производится дефаззификация с использованием базы знаний, которая строится на основе экспертных оценок.

$$\tau_{HSD} = FDEF\big(\tau(HSD)\big),$$

где $FDEF$ – нечеткая база знаний, построенная на основе экспертных оценок

Полученное значение используется для вычисления вероятности осуществления сценария атаки, в зависимости от времени

$$P(HSD)(t) = 1 - e^{-t/\tau_{HSD}},$$

где τ_{HSD} – дефаззифицированное значение прохода по сети,

t – время осуществления сценария

Результат данного шага определяет параметр $PTS(TS)$ для модели инцидентов, рассмотренной в предыдущем разделе.

Сценарии, описывающие ошибки, сбои и отказы трудно поддаются описанию моделями атак, так как зачастую это не этапы осуществления процесса, а наоборот – бездействие. Таким образом, для таких типов сценариев необходимо разработать модель, которая позволяет адекватно описать данные сценарии, учитывая их особенности реализации.

Моделирование ошибок и сбоев схоже по своей структуре, и основывается на показателях возможности осуществления процессов, характеризующих ошибки и неточности в работе системы. Для осуществления данного моделирования необходимо определить два параметра:

– показатель возможности. Данный параметр определяет вероятность того что ошибка или сбой возможна, и задается в диапазоне [0,1];

– время функционирования системы при наличии соответствующей ошибки, и измеряется в часах.

Вычисление вероятности осуществления сценария при этом выглядит следующим образом

$$P(TS) = 1 - e^{-\sigma t}.$$

где σ – коэффициент возможности ошибки, сбоя или отказа

t – время осуществления сценария

Физический смысл такой модели заключается в том, что она показывает насколько вероятность осуществления сценария зависит от возможности допу-

щения ошибки в выбранном интервале времени функционирования системы или ее элементов.

Например, если рассматривается сценарий «администратор сети допустил ошибку при настройке шлюза» (сценарий FGS) между внутренней и внешней сетью, возникает необходимость определить, насколько вероятно, что он осуществится течении суток при показателе возможности возникновения данной ошибки σ равной 0,7 и 0,3 (таблица 3.1).

Таблица 3.1 – Зависимость вероятности осуществления сценария

t	σ	$P(FGS)(t)$	σ	$P(FGS)(t)$
1	0,3	0,01	0,7	0,03
….	….	….	….	….
6	0,3	0,07	0,7	0,16
….	….	….	….	….
12	0,3	0,14	0,7	0,30
….	….	….	….	….
18	0,3	0,20	0,7	0,41
….	….	….	….	….
24	0,3	0,26	0,7	0,50

Логично, что при увеличении времени эксплуатации оборудования или других объектов информационно системы при наличии ошибки, вероятность осуществления данного сценария увеличивается и стремиться к единице. Наравне с этим максимальная оценка возможности не дает максимальной вероятности осуществления, что соответствует реальным условиям функционирования системы – даже полное отсутствие правил доступа на шлюзе не гарантирует моментального осуществления сценария.

Оценка сбоев системы основывается на таком же подходе к определению вероятности, однако меняется трактовка показателя возможности. Если при оценке сценариев ошибки данный показатель характеризует экспертную или случайную оценку внутренних показателей системы или ее пользователей, то

при определении вероятности сбоев, данный показатель характеризует не только состояние системы, но и внешние факторы.

К внешним факторам относятся природные катаклизмы, физические неполадки (вентиляция, электричество) и другие воздействия на систему. Для таких факторов показатель возможности является оценкой того, насколько возникновение данный фактор может воздействовать на осуществление сценария, и, может определяться экспертным путем, или на основе внешних источников информации (прогноз погоды, статистика перебоев в электроснабжении и др.)

При этом границы показателя сохраняются как в предыдущем случае и соответствуют диапазону [0,1].

3.3 Оценка угроз информационной безопасности

Как было определено ранее, угрозой является возможность того, что нарушение безопасности в информационной системе произойдет. Исходя из этого определения, можно увидеть, что угрозой является некоторый источник опасности, который способен привести к осуществлению сценариев в системе. Угрозы определяют внешнее или внутренне воздействие на систему, могут носить случайный или намеренный характер. Исходя из этого, были выявлены основные угрозы безопасности информационной системы (рисунок 3.2)

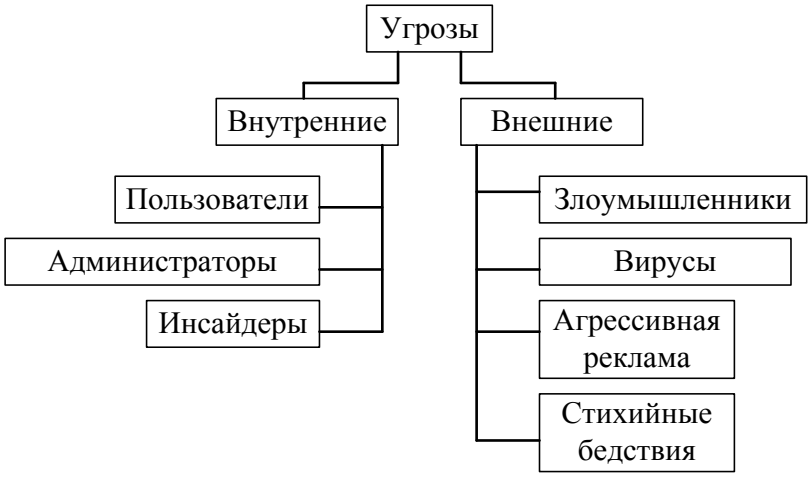


Рисунок 3.2 – Основные типы угроз

Тут представлены основные типы угроз в обобщенном виде. Многие из существующих угроз классифицированы и представлены в специализированных источниках, доступных для каждого кто намерен их изучить.

Как правило, угрозы ассоциируются со сценариями и инцидентами, и рассматриваются как единое целое. Однако данный подход не всегда оправдан в связи с отсутствием у систем моделирования атак такого понятия как источник события, что снижает достоверность оценки самого факта возникновения угроз. Однако на данные угрозы влияет множество факторов, которые способны снизить или увеличить вероятность их возникновения [63 – 64]. Данные факторы в дальнейшем играют роль уязвимостей системы, так как они определяют слабые места в работе системы и в использовании пользователями этой системы.

Совокупность таких факторов составляют множество элементов влияния на угрозу

$$PT(T_i) = \{\{Tf_1\}, \{Tf_2\}, \dots, \{Tf_n\}\}$$

где $PT(T_i)$ – вероятность возникновения угрозы,

$\{Tf_n\}$ – подмножество факторов, оказывающих влияние на $PT(T_i)$

Каждый элемент множества факторов является подмножеством однотипных элементов, что позволяет группировать схожие по свойствам факторы влияния. Это позволяет наглядно изображать структуру угрозы (рисунок 3.3) и упростить вычисление $PT(T_i)$.

Для оценки вероятности возникновения угрозы в системе, в работе предложен соответствующий метод, который состоит из четырех этапов.

На *первом* этапе определяются все факторы, которые могут оказать влияние на возникновение угрозы. Строится соответствующая структура и множество, где факторы группируются и представляются своими оценками $f_i(z_i)$. Каждая терминальная структура представляет оценку фактора, нетерминальная вершина является функцией свертки C_{vk} частных факторов.

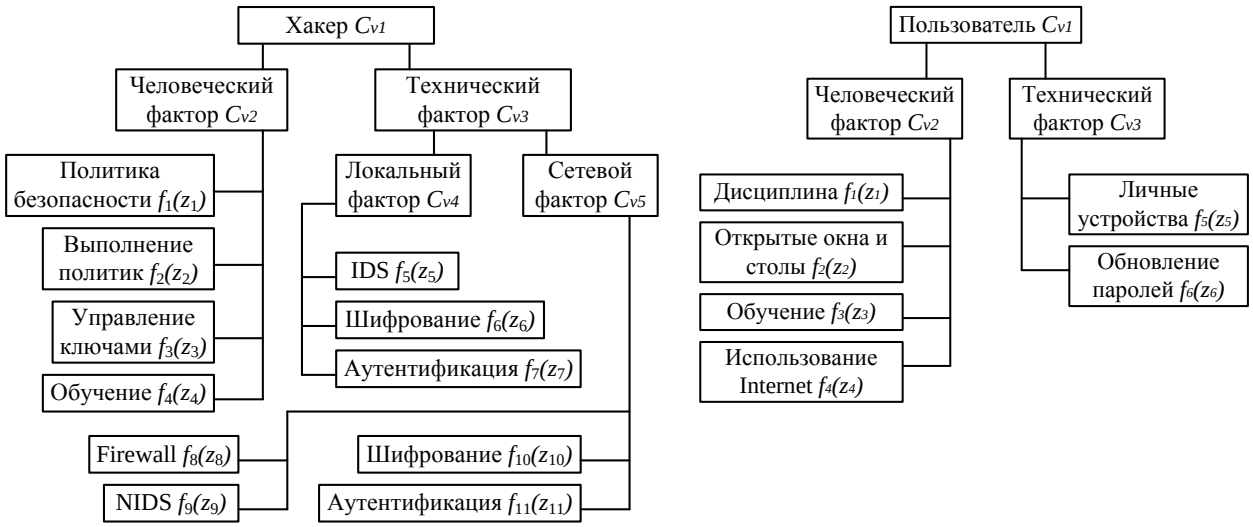


Рисунок 3.3 – Структура влияния на угрозы

На *втором* этапе каждый фактор получает экспертную оценку. Оценку необходимо нормировать, поэтому она задается с использованием коэффициента удовлетворенности:

$$f_i = 1 - e^{-\alpha t}$$

где α – коефициент удовлетворенности,

t – время функционирования рассматриваемого объекта

Коэффициент α определяет степень удовлетворенности состоянием системы, работой и навыками персонала и пр. Время t характеризует длительность работы объекта (устройство, система, актуальность информации и т. д.), который подвержен риску от рассматриваемой угрозы.

В рамках данного этапа выполняется ранжирование выявленных факторов. Это позволяет, на основе предпочтений экспертов, установить важность одних факторов перед другими, или определить наибольшее влияние совокупности факторов

$$Firewall \succ_C Аутентифікація \succ_C Шифрування \succ_C NIDS,$$

$$Firewall + Шифрування \succ_I Firewall + NIDS,$$

где $\succ_C$ – вотношение предпочтения между факторами,

$\succ_I$ – отношение взаимодействия пар факторов.

На основе данных предпочтений строится обучающее множество

Таблица 3.2 – Порядок факторов влияния в зависимости от предпочтений

Фактор / Набор оценок	*Firewall*	*Аутентифікація*	*Шифрування*	*NIDS*
A	0,8	0,85	0,9	0,9
B	0,85	0,8	0,9	0,9
C	0,7	0,8	0,6	0,4
D	0,7	0,8	0,4	0,6
E	0,5	0,8	0,4	0,6
F	0,5	0,8	0,6	0,4

При использовании аддитивных мер, параметр с большей оценкой имеет больший приоритет, однако, из таблицы 3.2 видно, что набор *A* имеет большее предпочтение, несмотря на меньшую оценку первого критерия.

На *третьем* этапе определяются нечеткие меры [84] для каждой нетерминальной вершины. Для этого используются полученные ранее оценки и значения предпочтений и взаимодействия. В результате получается множество нечеткой меры

$$v = [x_1, x_2, \dots, x_n], n = 2^k$$

где x_n – значения нечеткой меры

k – количество факторов, подчиненных вершине

Для удобства дальнейших вычислений, полученные значения подлежат обращения Мебиуса

$$m^v(A) = \sum_{B \subseteq \mathrm{A}} (-1)^{|A \setminus B|}\, v(B)$$

где B та A первичное и конечное множество значений соответственно

На *четвертом* этапе выполняется свертка оценок факторов с использованием нечеткого интеграла Шоке [70, 77] на основе коэффициентов m^v, вместо нечеткой меры

$C_{vi}(T_i) = p_1 f_1 + p_2 f_2 + \cdots + p_j f_j$, для агрегации факторов

$C_{vk}(T_i) = p_{k1} C_1 + \cdots + p_{ki} C_i$, для агрегации составных вершин

де f_j – экспертная оценка фактора,

p_j – коэффициент на основе m^v,

T_i – рассматриваемая угроза.

Результат данных действий определяет параметр $P(T)$, который необходим при оценки возможности возникновения инцидента безопасности.

3.4 Идентификация и оценка рисков

Все выявленные и оцененные элементы представляют собой последовательность параметров и действий, которые приводят к нарушению свойств актива, и, соответственно, к нарушению безопасности деятельности организации, осуществляющей информационную деятельность.

Как было определено, риском является возможность ущерба активам от соответствующих инцидентов безопасности. В пункте 2.3 было показано, что каждому активу рассматриваемой системы может сопоставляться несколько инцидентов безопасности, каждый из которых влияет на актив с соответствующим отношением влияния. Очевидно, что инцидент, влияющий на несколько

активов, способствует различной степени ущерба для каждого из них, и, соответственно, формирует различные риски для активов (рисунок 3.4).

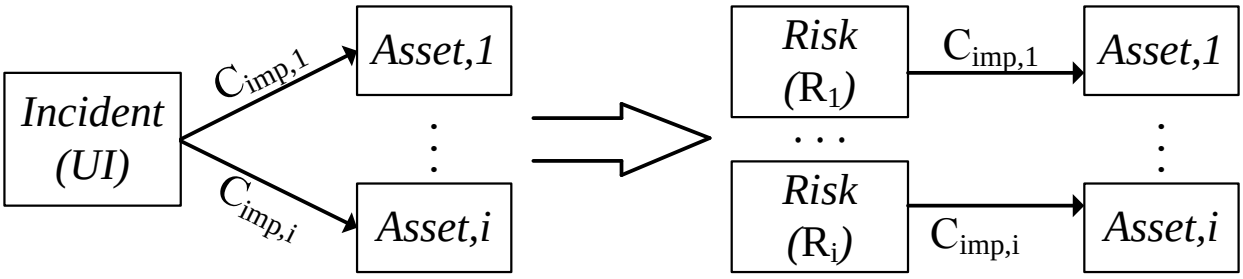


Рисунок 3.4 – Формирование рисков для активов

Для идентификации и оценки риска в работе предложен соответствующий метод, состоящий из трех этапов.

На *первом* этапе определяются риски информационной безопасности. На основе подхода представленного на рисунке 3.4, формируется множество рисков для активов, определяемого парой параметров

$$R_i = \{P(UI_i), C_{imp,i}\},$$

где $P(UI)$ – оценка -го инцидента,

C_{imp} – i-я оценка ущерба от инцидента

Оценка инцидента характеризуется нормированным значением и представляется числами из диапазона [0,1]. Оценка ущерба от актива определяется значением терм-множеством $T(Impact)$. Оценка риска осуществляется, по аналогии с оценкой актива, с использованием соответсвующего терм-множества для рисков [56, 91]:

$$T(Risk) = \{\text{"низкий"}, \text{"неопасный"}, \text{"средний"}, \text{"опасный"}, \text{"высокий"},\}$$

При этом, строится структура рисков, которая описывает влияние на актив (рисунок 3.5)

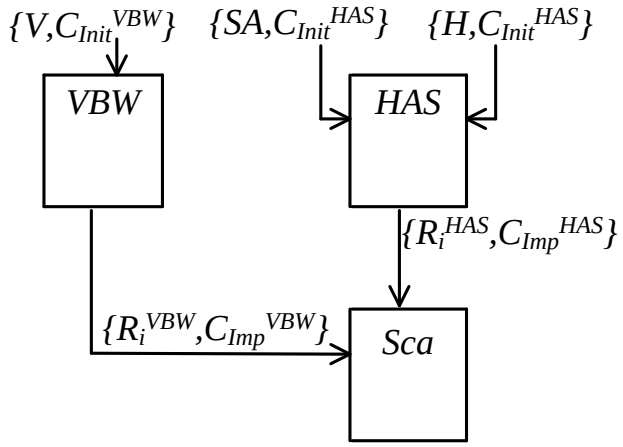


Рисунок 3.5 – Структура взаимодействия рисков и активов

Как видно из структуры, активу ставятся в соответствие все идентифицированные риски, а каждому риску ставятся в соответствие угрозы, возникновение которых привело к конкретному риску.

Каждый блок риска определяется двумя составляющими, которые формируются в соответствующих базах знаний (рисунок 3.6)

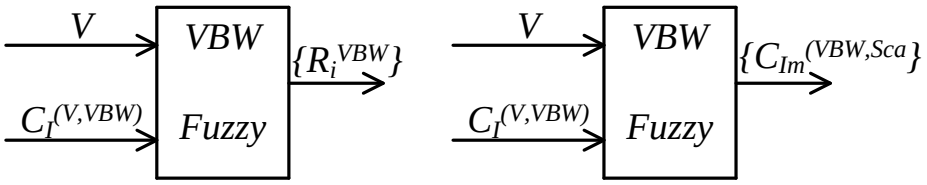


Рисунок 3.6 – Базы знаний для риска

Базы знаний хранят понятия и правила для описания ущерба активу от риска, которые определяются на последнем этапе метода. Для этого использована онтология OWL, в которой были определены все необходимые для анализа рисков элементы. Данная онтология разработана в работах [76, 92 – 93] и доработана для использования в решении задач поставленных в диссертации. В онтологии содержатся следующие понятия:

– класс Scenario, который представляет все сценарии представляемые в построенных иерархических моделях;

– класс Diagrams, который позволяет представлять все возможные в рамках методологии диаграммы. Для каждого отдельного понятия введен свой підклас;

– класс Vulnerability, который позволяет представлять все возможные увязвимости ВС;

– класс Unwanted_incident, который позволяет представлять все возможные нежелательные инциденты ВС;

– класс Threat, который позволяет представлять все возможные угрозы инциденты ВС;

– класс Node (класс введенный автором), который позволяет представлять все возможные дополнительные узлы, которые необходимы для иерархического описания влияния на актив;

– класс LinkNode (класс введенный автором), который позволяет представлять все возможные дополнительные связи между узлами, которые необходимы для иерархического описания влияния на актив.

На *втором* этапе проводится классификация оценок инцидентов и ущерба с целью получения значения риска для выбранного актива [20, 75, 94]. Для осуществления данного этапа проводится нечеткая кластеризация по двум параметрам. Учитывая известные проблемы методов кластеризации [25], а также возможной большой погрешностью при точном задании количества кластеров, равном количеству переменных, целесообразно использовать большое количество кластеров, с дальнейшим их объединением до достижения адекватного количества для оценки риска.

Результатом выполнения второго этапа является множество центров кластеров V_i и множество степеней принадлежности M_i к каждому кластеру. При большом количестве полученных центров, представляется сложным процесс определения конечного уровня риска для актива. Следовательно, необходимо произвести объединение кластеров, пока не будет достигнуто количество кластеров, соответствующее количеству термов, описывающих уровень риска.

Предполагая, что размеры исходных кластеров неодинаковы, адекватным считаются методы взвешенного попарного среднего, который позволяет учесть размеры кластеров.

На *третьем* этапе осуществляется обработка полученных кластеров и соответствующих им значений риска. Основываясь на данных параметрах, строятся нечеткие правила для базы знаний , которые определяют принадлежность значений инцидента и ущерба к определенному уровню риска

$$\bigcup_{1}^{k}[\bigcap_{1}^{q}(x_i = a_i, y_i = b_i)] \rightarrow R = d_j,$$

где x_i, y_i – входные параметры (инциденты та ущерб),

a_i, b_i – соответствующие оценки инцидентов та ущерба,

k – количество строк (конъюнкций) правил,

q – количество пунктов каждой строки правила,

d_j – соответствующие термы значений оценки уровня риска

На основе полученных результатов классификации и нечетких правил можно определить значение уровня риска на основе его входных параметров. Для удобства кластеризации, лингвистическим термам отношения влияния были сопоставлены непересекающиеся бальные оценки (рисунок 3.7)

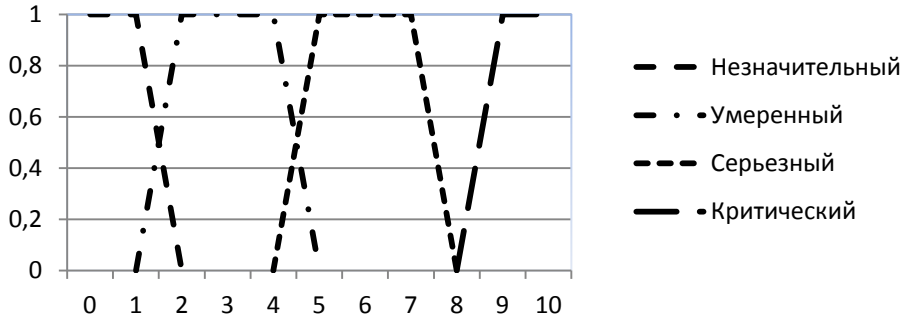


Рисунок 3.7 – Соответствие бальных оценок лингвистическим термам

На основе полученных числовых оценок строится соответствие лингвистическим термам, которые определяют уровень риска (таблица 3.3).

Таблица 3.3 – Оценка уровня риска

C_{imp}^{VBW}	$PUI(VBW)$	R^{VBW}	C_{imp}^{HAS}	$PUI(HAS)$	R^{HAS}
2,8	0,315	Низкий	1,4	0,42	Неопасный
3,4	0,479	Средний	6,2	0,979	Опасный
3,4	0,662	Средний	4,8	0,935	Опасный
7,8	0,055	Средний	1,2	0,029	Низкий
9,2	0,536	Опасный	5	0,359	Неопасный
0,6	0,079	Низкий	1	0,418	Неопасный
6,8	0,945	Высокий	8,2	0,406	Средний
0,9	0,986	Средний	9	0,567	Опасный
5,5	0,437	Средний	2	0,951	Средний
6,6	0,795	Опасный	3,3	0,908	Опасный
9,9	0,767	Высокий	9,7	0,848	Высокий
4,7	0,582	Опасный	0,2	0,79	Средний
9,4	0,866	Высокий	4,1	0,795	Средний
8,8	0,496	Опасный	1,4	0,236	Низкий
5,9	0,16	неопасный	7	0,24	Средний

При этом всегда возможно проследить, при каких параметрах моделей, было получено соответствующее значение риска, определив какие уязвимые места системы (факторы влияния на угрозу) приводят к такому уровню риска. Это позволяет экспертам определять, в дальнейшем, меры по обработке риска [85, 87].

3.5 Выводы

В данном разделе были определены модели, позволяющие осуществить оценку процессов в информационной системе, которые приводят к инцидентам безопасности, а также оценить причины возникновения данных процессов и событий. При этом, достигнуто следующее:

– определены типы сценариев, которые приводят к инцидентам и разработаны соответствующие модели оценки вероятности реализации данных сценариев. Предложено два подхода – на основе сетей Петри с нечеткими пара-

метрами для атак, и на основе коэффициентов возможности для сбоев и ошибок;

– разработан метод моделирования атак на основе нечетких временных показателей, оценивающий вероятность реализации сценария атаки;

– разработан метод оценки угроз информационной безопасности, позволяющий оценивать вероятность возникновения опасных событий на основе факторов влияния, которые характеризуют уязвимее места информационной системы и ее пользователей;

– получил дальнейшее развитие метод оценки риска на основе лингвистических переменных и нечеткой кластеризации;

– разработаны нечеткие базы знаний, позволяющие осуществлять оценку элементов риска на основе опыта экспертов и статистических данных.

РАЗДЕЛ 4
ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1 Информационная технология анализа рисков

Результаты разработки моделей и методов в предыдущих главах позволили объединить их в единую информационную технологию (рисунок 4.1), которая состоит из десяти этапов.

На первом этапе с участием группы экспертов и уполномоченных участников анализа рисков определяется множество активов информационной системы, подлежащих защите. Определяется взаимосвязь между активами с целью выявления отношений ущерба для активов системы.

На втором этапе группой экспертов определяются инциденты, сценарии и угрозы, которые способны нанести вред выявленным активам. На основе этих данных строится информационная структура элементов риска для каждого актива, которая позволяет структурировать влияние выявленных элементов на каждый актив.

На третьем этапе группой экспертов с участием уполномоченных участников, определяются лингвистические переменные для всех типов отношений, активов и рисков.

На четвертом этапе проводится оценка вероятности возникновения угроз. С привлечением администраторов системы, экспертом (мы) определяется множество факторов, которые способствуют возникновению угрозы. Производится группировка этих факторов, их ранжирование, и исчисляется общая оценка каждой выявленной угрозы.

На пятом этапе проводится моделирование и оценка вероятности осуществления выявленных сценариев. При возможном участии администраторов,

определяются этапы сценариев и их характеристики осуществления. Определяется множество мест уязвимости. При необходимости проводится имитационное моделирование соответствующего сценария.

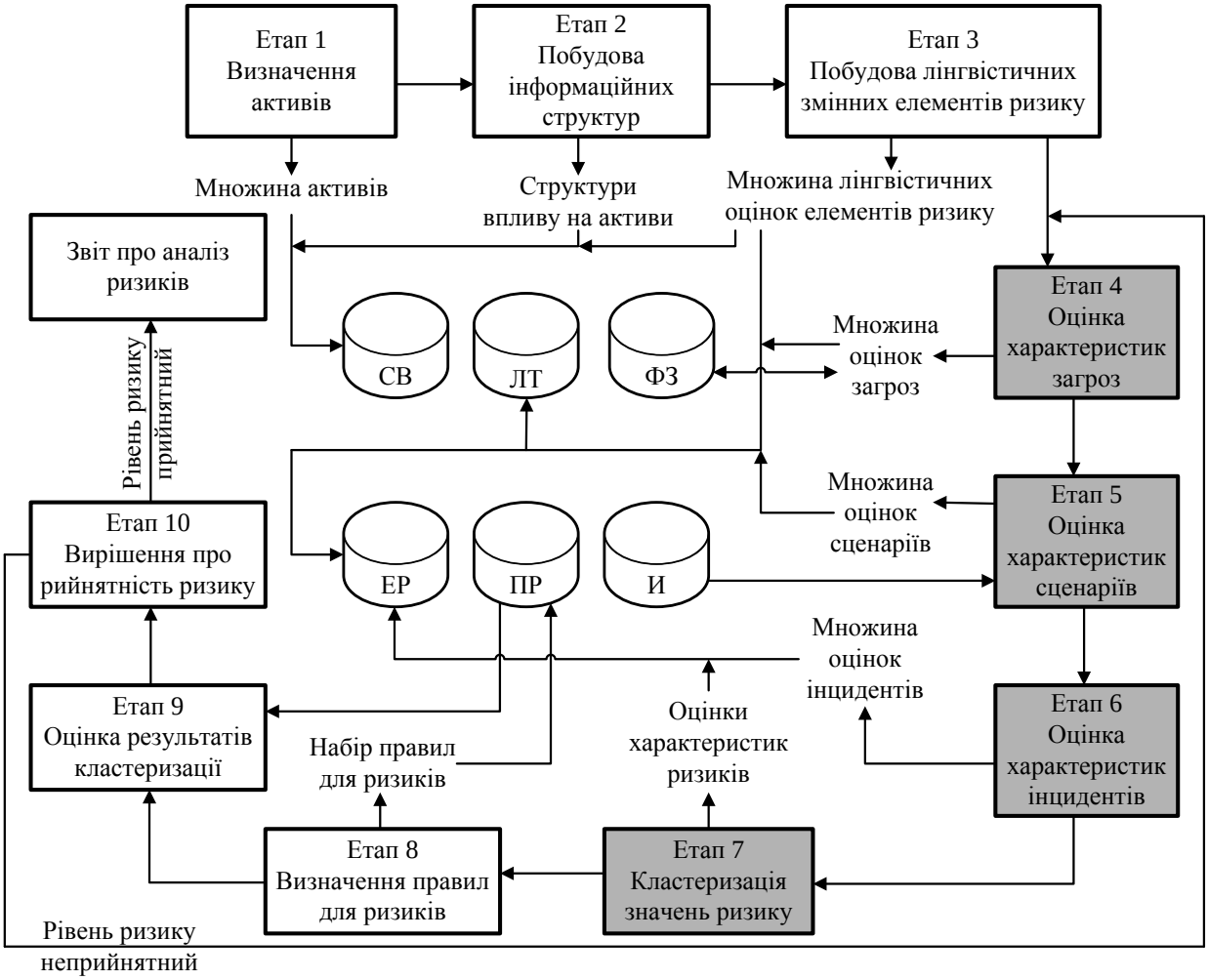


Рисунок 4.1 – Информационная технология анализа рисков: СВ – БД структур влияния на активы, ЛТ – БД лингвистических термов, ФЗ – БД факторов влияния на угрозы, ЕР – БЗ элементов риска; ПР – БЗ правил для рисков; И – БЗ имитационного моделирования

На шестом этапе проводится оценка вероятности возникновения инцидентов с использованием определенных в работе моделей инцидентов.

На седьмом этапе проводится кластеризация оценок вероятности возникновения инцидентов и ущерба от них, что позволяет определить рисков по соответствующим уровням для каждого актива информационной системы. Пер-

воначальное количество кластеров объединяется с количеством, определенной количеством термов соответствующей лингвистической переменной.

На восьмом этапе на основе полученной кластеризации строятся соответствующие правила для базы знаний рисков, которые связывают входные данные инцидентов и ущерба от них с соответствующим уровнем риска.

На девятом этапе осуществляется сравнительная оценка рисков. Определяется возможность приемлемого или неприемлемого уровня рисков для каждого актива в соответствии с целями менеджмента рисков.

На десятом этапе принимается решение о приемлемости уровня риска. Если уровень приемлем, готовится отчет о результатах анализа рисков, если уровень риска неприемлем, осуществляется возврат к этапу 4.

4.2 Программно-инструментальные средства для анализа рисков

При реализации разработанной технологии использовался комплекс программных и инструментальных средств, благодаря использованию которых возможно осуществить все этапы технологии. Структура программного комплекса представлена на рисунке 4.2. В ходе разработки комплекса использовались свободно распространяемые среды программирования и прикладные пакеты.

Модуль интерфейса осуществляет интерактивный обмен данными между модулями системы, а также с оператором. Также осуществляется ввод/вывод данных при идентификации элементов риска, параметризации моделей, выводе промежуточных результатов, отчетов и др. Форматом данных для обмена между различными модулями прият язык разметки документов XML. Который позволяет оперировать документами в виде текста, таблиц и пр., а также поддерживается используемыми программными средствами при реализации модулей комплекса.

Модуль синтеза структур взаимодействия позволяет графически структурировать выявленные элементы риска и определять взаимодействие между ни-

ми. Разработанные структуры заносятся в специальную базу данных структур влияния.

Модуль оценки параметров осуществляет вычисление значений моделей для всех элементов риска. Блок расчета нечетких мер представляет собой специализированную библиотеку kappalab для расчета нечетких мер по методу MACBETH. Вычисление основывается на количестве входных параметров модели и их ранжировании. Также в данном блоке осуществляется обращение Мебиуса для значений нечеткой меры, что позволяет в дальнейшем вычислять нечеткий интеграл в виде линейной функции.

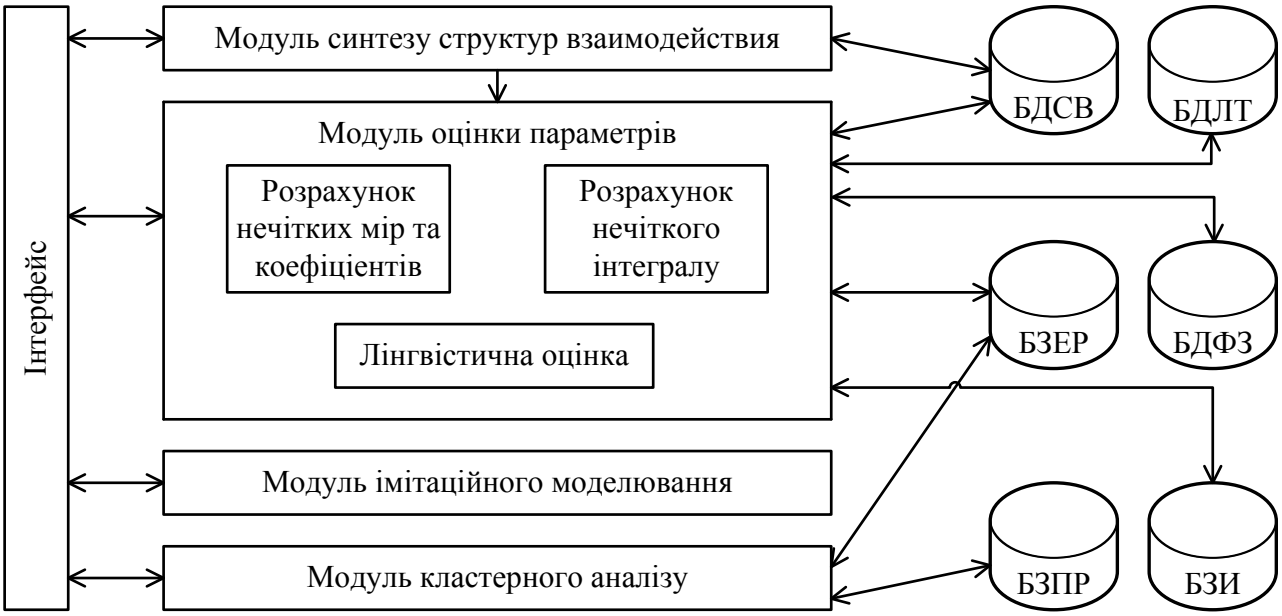


Рисунок 4.2 – Программно-инструментальный комплекс: СВ – БД структур влияния на активы, ЛТ – БД лингвистических термов, ФЗ – БД факторов влияния на угрозы, ЕР – БЗ элементов риска; ПР – БЗ правил для рисков; И – БЗ имитационного моделирования

Расчет нечеткого интеграла производит вычисление итоговой оценки соответствующего объекта на основе его параметров и полученных коэффициентов в результате обращения Мебиуса. Расчет реализован на языке Python с последующим преобразованием результатов в формат XML.

Лингвистическая оценка применяется при работе с активами, отношениями и рисками. Позволяет осуществлять оценивание свойств данных объектов с точки зрения естественного языка.

Модуль оценки параметров взаимодействует с базой данных структур влияния, принимая выявленные элементы риска для дальнейшего оценивания. В процессе оценивания элементов риска, модуль взаимодействует с базами данных лингвистических термов и факторов угроз и базами знаний элементов риска и имитационного моделирования, из которых осуществляется извлечение необходимых значений, или наоборот загрузка новых результатов моделирования.

Модуль имитационного моделирования позволяет осуществлять имитацию сценариев угроз в реальных условиях, с целью получения экспериментальных значений, которые можно использовать при обучении в системе нечеткого логического вывода при моделировании сценариев. Модуль реализован на языке C++ и содержит большинство представленных в работе сценариев, описанных сетями Петри.

Модуль кластерного анализа осуществляет кластеризацию значений инцидентов и ущерба от них и позволяет производить классификацию полученных значений рисков. Модуль позволяет осуществлять классификацию по выбранному количеству уровней риска, а также осуществлять классификацию по степени приемлемости уровня риска, основываясь на оценках свойств соответствующего актива.

Базы данных и знаний, используемых в комплексе, позволяют накапливать информацию о проведенных процессах идентификации, анализе и оценке рисков, что позволяет использовать опыт экспертов при построении систем защиты информации или повторном анализе функционирующей системы.

В комплексе используются три основных базы данных и три базы знаний.

БД структур влияния на активы накапливает описания полученных структур для активов. Также данная БД позволяет использовать шаблонные структуры при идентификации рисков.

БД лингвистических термов содержит в себе типовые лингвистические термы в области информационной безопасности и позволяет пополнять ее новыми термами, сформулированными участниками анализа рисков.

БД факторов влияния на угрозы содержит типовые факторы, которые способны привести к возникновению угрозы. Пополнение данной БД осуществляется на основе анализа соответствующих источников информации (отчеты лабораторий, специальные сайты уязвимостей и т. д.) или на основе опыта участников процесса анализа рисков.

Управление базами данных осуществляется с использованием свободной реляционной системы управления MySQL

БЗ элементов риска содержит сущности элементов риска и отношения между ними. Данная база знаний позволяет строить иерархические взаимосвязи между объектами и накапливать опыт по идентификации и изучению данных элементов.

БЗ правил для рисков позволяет накапливать знания о правилах рисков и использовать их при изучении рисков в ходе повторного анализа информационной системы, или в дальнейшей практике участников риска.

БЗ имитационного моделирования позволяет накапливать знания о сценариях угроз и используется при обучении с применением системы нечеткого логического вывода, когда осуществляется обработка входных данных моделей.

4.3 Использование информационной технологии в анализе рисков

Разработанные информационная технология и средства анализа рисков позволили осуществить экспериментальные расчеты для оценки риска в реальных условиях функционирования системы.

4.3.1 Идентификация элементов риска и экспериментальная система

При идентификации активов было выявлено, что на рассматриваемый актив, может быть оказано влияние двух активов:

– Uda – личные данные пользователя. Нарушение конфиденциальности пользовательских идентификаторов может нанести ущерб рассматриваемому активу;

– Sa - нарушение доступности серверов определенно приводит к ущербу сервисам, предоставляемым данными серверами.

Исходя из данных утверждений, следует произвести ранжирование важности активов, для дальнейшего анализа. В ходе данного ранжирования, основываясь на способности нанести вред активу, были определены следующие оценки:

– актив Sca получил оценку «высокая». Доступность сервисов важна, однако, учитывая бесплатность данного сервиса, критичная оценка не устанавливается;

– актив Sa получил оценку «высокая». Нарушение свойств данного актива критично для сервисов;

– актив Uda получил оценку «умеренная». Нарушение свойств данного актива приводит к ущербу Sca с меньшей вероятностью, чем Sa.

В соответствии с полученной идентификационной структурой, модель данного актива выглядит следующим образом

$$F(A) = \{C_{VBW}^{imp}, C_{HAS}^{imp}, C_{Sa}^{harm}, C_{Uda}^{harm}, PA(Sa), PA(Uda), P(VBW), P(HAS)\},$$

Следующим шагом определяются множество элементов, которые приводят к нарушению безопасности системы. Для идентификации элементов риска были приглашены 5 экспертов, которые, основываясь на статистических данных и собственном опыте, выявили три инцидента, четыре сценария и три угрозы, которые могут нанести ущерб выбранному активу:

– инциденты:

а) VBW – вирус заблокировал работу системы;

б) HAS – злоумышленник получил доступ к серверу;

в) HAR – злоумышленник получил доступ к управлению сервисами;

– сценарии:

а) VIA – инфицирование приложений вирусом;

б) FAS – ошибка в настройках приложения;

в) FSM – ошибка в управлении сервисами;

г) HSS – запуск злоумышленником сценариев на сервере;

– угрозы:

а) вирус;

б) администратор сервисов;

в) злоумышленник.

В качестве испытуемой информационной системы выступала лаборатория, в состав которой входили 14 пользовательских станций 1 сервер, 1 маршрутизатор и 3 коммутатора, что позволило организовывать произвольное количество подсетей и переконфигурировать коммуникационную структуру системы.

Оценка активов производилась на основе приоритетов владельца активов и экспертной оценки взаимодействия активов. Основным рассматриваемым активом является «доступность сервисов» и был оценен как «высокая». Кроме того, на актив оказывают воздействие активы «доступность личных данных» и «доступность сервера». Доступность личных данных связана с конфиденциальностью пользовательских данных и оценена как «умереная». Доступность сервера напрямую связана с доступностью сервисов и оценена как «высокая».

Отношения вреда между данными активами установлены исходя из их оценок:

$$C_i^{harm} = A(Uda) \xrightarrow{Harm} A(Sca) = \{\text{"малый"}\},$$

$$C_i^{harm} = A(Sa) \xrightarrow{Harm} A(Sca) = \{\text{"крайний"}\}.$$

Сервисы предоставляются на бесплатной основе, следовательно нет экономической ответственности перед пользователями системы. Исходя из этого,

отношение ущерба определяется временем восстановления доступности сервиса:

$T_1(Impact) = \{$"незначительный"$\}$ – необходимое время восстановления доступности составляет [20 – 45] минут;

$T_2(Impact) = \{$"умеренный"$\}$ – необходимое время восстановления доступности составляет [45 - 90] минут;

$T_3(Impact) = \{$"серьезный"$\}$ – необходимое время восстановления доступности составляет [90 - 180] минут;

$T_4(Impact) = \{$"критический"$\}$ – необходимое время восстановления доступности составляет более 3 часов;

$T_5(Impact) = \{$"непорпавимый"$\}$ – сервис не подлежит восстановлению.

4.3.2 Оценка угроз информационной системы

Необходимо определить факторы, влияющие на возникновение трех угроз информационной системе.

Для угрозы «вирус» определены следующие факторы:

– человеческий фактор:

а) «почта» – корректное использование постовых систем (игнорирование подозрительных писем, настройка спама и т. п.);

б) «WEB» – корректное использование Интернет ресурсов (отказ от посещения сомнительных ресурсов);

в) «личные устройства» – использование проверенных и не зараженных мобильных устройств, имеющих доступ к системе;

– технический фактор:

а) «антивирус» – поддержание антивирусной системы в актуальном состоянии (обновление системы, обновление баз вирусов);

б) «обновления» – контролированное обновление операционных систем, используемых в сети;

в) «NIDS» – использование сетевой системы обнаружения вторжений;

Для угрозы «администратор сервисов» выявлены следующие факторы:

– человеческий фактор:

а) «квалификация» – навыки администратора в области управления информационными сервисами;

б) «конфиденциальность» – сохранение идентификационных данных в тайне;

в) «выполнение политик» – следование установленным нормам использования системы и ее составляющих;

– технический фактор:

а) «управление сеансами» – установление параметров, которые определяют порядок использования сервисов системы;

б) «аудит» – регулярный мониторинг использования сервисов и связного с ними оборудования;

в) «шифрование» – использование криптографических средств при установлении, использовании и закрытии сеансов связи;

г) «аутентификация» – корректное управление учетными записями и паролями пользователей сервисов.

Для угрозы «злоумышленник» установлены следующие факторы:

– человеческий фактор:

а) «политика безопасности» – насколько грамотно составлена политика безопасности и насколько она выполняется;

б) «обучение» – насколько грамотно используются ресурсы системы;

в) «конфиденциальность» – насколько корректно обращение пользователей с идентификационными данными;

– технический фактор (локальный):

а) «IDS» – использование системы обнаружения вторжений;

б) «аутентификация» – ограничение доступа к оборудованию;

– технический фактор (сетевой):

а) «Firewall» – корректность настройки межсетевого экрана;

б) «NIDS» – использование сетевой системы обнаружения вторжений;

в) «шифрование» – криптографическая защита передаваемых данных;

г) «аутентификация» – ограничение внешнего доступа к системе.

Следующим этапом необходимо провести оценку выявленных факторов угроз. Для этого задается множество параметров α, которые определяют показатель удовлетворенности, и рассчитывается оценка каждого частного фактора. В рамках эксперимента были рассмотрены 10 вариантов различных состояний факторов.

На основе полученных оценок и их предпочтений вычисляется нечеткая мера для всех обобщенных факторов и угрозы в целом, с последующим обращением Мебиуса.

Для угрозы «вирус»:

– угроза = [0, 0.37, 0.27, 1];

– технический фактор = [0, 0.62, 0.69, 0.43, 0.34, 0.68, 0.88, 0.15, 0.36, 0.55, 0.36, 0.13, 0.52, 0.37, 0.51, 1];

– человеческий фактор = [0, 0.57, 0.18, 0.19, 0.56, 0.08, 0.61, 1].

Для угрозы «Администратор сервисов»:

– угроза = [0, 0.87, 0.1, 1];

– технический фактор = [0, 0.1, 0.36, 0.66, 0.05, 0.9, 0.89, 1];

– человеческий фактор = [0, 0.46, 0.6, 0.32, 0.2, 0.64, 0.78, 1]

Для угрозы «Злоумышленник»:

– угроза = [0, 0.5, 0.16, 1];

– технический фактор = [0, 0.17, 0.35, 1];

– технический фактор (сетевой) = [0, 0.85, 0.65, 0.16, 0.22, 0.24, 0.21, 0.56, 0.38, 0.0, 0.47, 0.62, 0.55, 0.88, 0.57, 1];

– технический фактор (локальный) = [0, 0.16, 0.37, 1];

– человеческий фактор [0, 0.88, 0.43, 0.27, 0.97, 0.11, 0.63, 1].

Далее проводится расстановка факторов в порядке предпочтения, для определения итоговых коэффициентов при каждой оценке фактора

Для угрозы «вирус»

$$почта \succ_C личные\ учтройства \succ_C WEB,$$
$$NIDS \succ_C антивирус \succ_C обновления,$$
$$человеческий\ фактор \succ_C технический\ фактор.$$

Для угрозы «администратор сервисов»

$$квалификация \succ_C конфиденциальность \succ_C выполнение\ политик,$$
$$управление\ сеансами \succ_C аудит \succ_C аутентификация \succ_C шифрование,$$
$$человеческий\ фактор \succ_C технический\ фактор.$$

Для угрозы «злоумышленник»

$$обучение \succ_C политика\ безопасности \succ_C конфиденциальность,$$
$$IDS \succ_C аутентификация,$$
$$Firewall \succ_C NIDS \succ_C аутентификация \succ_C шифрование$$
$$сетевой\ фактор \succ_C локальный\ фактор$$
$$технический\ фактор \succ_C человеческий\ фактор$$

Получив данные коэффициенты, вычисляются оценки каждой угрозы

Используя все полученные значения и приоритеты возможен расчет итоговых оценок угроз:

Угроза «вирус»:

$$C_{v1}^V = (m_3 + m_{13})f3 + (m_2 + m_{12} + m_{23} + m_{123})f2 + m_1 f1 =$$
$$(0.57 + 0.08) * 0.03 + (0.18 + 0.34 + 0.61 + 1) * 0.01 + 0.6 * 0.03 = 0.01,$$
$$C_{v2}^V = (m_3 + m_{13} + m_{23} + m_{123})f3 + (m_2 + m_{23})f2 + m_1 f1 =$$
$$(0 + 0.08 + 0.61 + 1) * 0.03 + (0.18 + 0.56) * 0.01 + 0.57 * 0.01 = 0.08,$$
$$C_v^V = (m_2 + m_{12})f2 + m_1 f1 = (0.27 + 1) * 0.09 + 0.37 * 0.06 = 0.15.$$

Угроза «администратор сервисов»:

$$C_{v1}^{SA} = (m_3 + m_{13} + m_{23} + m_{123})f3 + (m_2 + m_{23})f2 + m_1 f1 =$$
$$(0 + 0.64 + 0.78 + 1) * 0.03 + (0.6 + 0.2) * 0.02 + 0.46 * 0 = 0.08,$$
$$C_{v2}^{SA} = m_1 f1 + (m_2 + m_{12})f2 + (m_3 + m_{13} + m_{23} + m_{34} + m_{123} + m_{134} + m_{234} + m_{1234})f_3 + (m_4 + m_{14} + m_{24} + m_{124})f_4 = 0.62 * 0.03 + (0.69 + 0.68)0.03 + (0.43 + 0.88 + 0.36 + 0.13 + 0.53 + 0.51 + 1) * 0.02 + (0.34 + 0.15 + 0.55 + 0.52) = 0.13,$$
$$C_v^{SA} = m_1 f1 + (m_2 + m_{12})f2 = 0.87 * 0{,}08 + (0.1 + 1) * 0.13 = 0.21$$

Угроза «злоумышленник»:

$$C_{v1}^{H} = (m_1 + m_{12})f1 + m_2 f2 + (m_3 + m_{13} + m_{23} + m_{123})f_3 =$$
$$(0.88 + 0.97) * 0{,}06 + 0.43 * 0{,}04 + (0.27 + 0.11 + 0.63 + 1) * 0.07 = 0.27.$$
$$C_{v2}^{H} = m_1 f_1 + (m_2 + m_{12})f_2 = 0.16 * 0.04 + (0.37 + 1) * 0.04 = 0.06$$
$$C_{v3}^{H} = m_1 f1 + (m_2 + m_{12})f2 + (m_3 + m_{13} + m_{23} + m_{34} + m_{123} + m_{134} + m_{234} + m_{1234})f_3 + (m_4 + m_{14} + m_{24} + m_{124})f_4 = 0.85 * 0.10 + (0.65 + 0.21) * 0.11 + (0.24 + 0.21 + 0.38 + 0.47 + 0.62 + 0.88 + 0.57 + 1) * 0.02 + (0.16 + 0.56 + 0.0 + 0.55) = 0.39,$$
$$C_{v4}^{H} = m_1 f_1 + (m_2 + m_{12})f_2 = 0.17 * 0.39 + (0.35 + 1) * 0.06 = 0.14$$
$$C_v^{H} = m_1 f_1 + (m_2 + m_{12})f_2 = 0.14 * 0.5 + (0.16 + 1) * 0.27 = 0.39$$

Исходя из данных вычислений, получаем множество оценок для каждой выявленной угрозы:

$$PT(V) = \{0.15, 0.50, 0.23, 0.53, 0.53, 1.38, 1.88, 2.12, 1.79, 2.46\},$$
$$PT(SA) = \{0.21, 0.89, 1.07, 1.72, 1.69, 1.78, 0.75, 187, 3.86, 4.50\},$$
$$PT(H) = \{0.09, 0.39, 0.59, 0.35, 0.88, 0.99, 0.34, 1.73, 0.92, 1.51\}.$$

Данные оценки являются входными параметрами $PT(T)$ для вычисления оценки вероятности осуществления сценариев, и характеризуют возможность возникновения данных сценариев.

4.3.3 Оценка возможности осуществления сценариев

Оценка вероятности осуществления сценария зависит от четырех основных параметров:

– оценка угрозы;

– оценка уязвимостей;

– отношение инициализации сценария угрозой;

– вероятность возникновения сценария.

Первый параметр получен в пункте 4.3.1. Оценка уязвимостей строится на основе выявленных факторов угроз, которые характеризуют слабые места системы. Выявленные факторы можно детализировать, с целью уточнения характера уязвимости, оценив при этом каждый новый параметр. Оценки параметров строятся на основе оценки фактора, как результата вычисления интеграла. Соответственно вычисляются соответствующие коэффициенты Мебиуса и определяются оценки параметров при этих коэффициентах.

Вычисление вероятности сценария заключается в моделирования его процессов, как было показано в предыдущем разделе. Соответственно, необходимо решить 4 задачи, две из которых описывают атаки, две описывают ошибки.

Для решения задач определения вероятности атак, необходимо определить этапы и их нечеткие временные характеристики. Для сценария VIA такими параметрами являются:

– $\tau_{11}(VIA) = [2, 5]\text{с}, \Delta = 0.15$ с – среднее время запуска приложения;

– $\tau_{21}(VIA) = [5, 10]c, \Delta = 0.25$ с – среднее время подготовки пользователя;

– $\tau_{32}(VIA) = [2, 10]\text{с}, \Delta = 0.4$ с – среднее время работы приложения до инфицирования вирусом.

Итоговая вероятность равна

$$\tau_1(VIA) = \frac{\tau_{11}(VIA)^2 + \tau_{11}(VIA)\tau_{21}(VIA) + \tau_{21}(VIA)^2}{\tau_{11}(VIA) + \tau_{21}(VIA)} =,$$

$$\tau = \tau_1(VIA) + \tau_{32}(VIA),$$

$$\tau_{VIA} = FDEF\big(\tau(VIA)\big),$$

$$P(VIA)(t) = 1 - e^{-t/\tau_{VIA}}.$$

Для сценария HSS определены следующие параметры:

– $\tau_{11}(HSS) = [0.1, 0{,}4]\text{с}, \Delta = 0.03$ с – среднее время передачи пакетов серверу;

– $\tau_{21}(HSS) = [0.2, 0.5]c, \Delta = 0.01$ с – среднее время перехвата пакетов злоумышленником;

– $\tau_{32}(HSS) = [1, 3]\text{с}, \Delta = 0.2$ с – среднее время модификации пакетов;

– $\tau_{43}(HSS) = [1, 5]\text{с}, \Delta = 0.15$ с – среднее время срабатывания сценария на сервере.

Итоговая вероятность равна

$$\tau_1(HSS) = \frac{\tau_{11}(HSS)^2 + \tau_{11}(HSS)\tau_{21}(HSS) + \tau_{21}(HSS)^2}{\tau_{11}(HSS) + \tau_{21}(HSS)},$$

$$\tau = \tau_1(HSS) + \tau_{32}(HSS) + \tau_{43}(HSS),$$

$$\tau_{VIA} = FDEF\big(\tau(HSS)\big),$$

$$P(HSS)(t) = 1 - e^{-t/\tau_{HSS}}.$$

Сценарии FAS и FSM определяют ошибки в работе администратора, и соответственно определяются коэффициентом возможности σ, который определен для сценария FAS равным $\sigma = 0.35$, а для сценария FSM равным $\sigma = 0.55$.

Соответствующие результаты вычислений вероятностей представлены в таблице 4.1.

Таблица 4.1 – Зависимость вероятности осуществления сценария

t	σ	$P(FAS)(t)$	σ	$P(FSM)(t)$
1/24	0.35	0.01	0.55	0.02
….	….	….	….	….
5/24	0.35	0.07	0.55	0.11
….	….	….	….	….
10/24	0.35	0.14	0.55	0.20
….	….	….	….	….
14/24	0.35	0.18	0.55	0.27
….	….	….	….	….
17/24	0.35	0.22	0.55	0.32
….	….	….	….	….
20/24	0.35	0.25	0.55	0.37
….	….	….	….	….
24/24	0.35	0.30	0.7	0.42

Рост вероятности реализации сценария в течении суток представлен на рисунке 4.3.

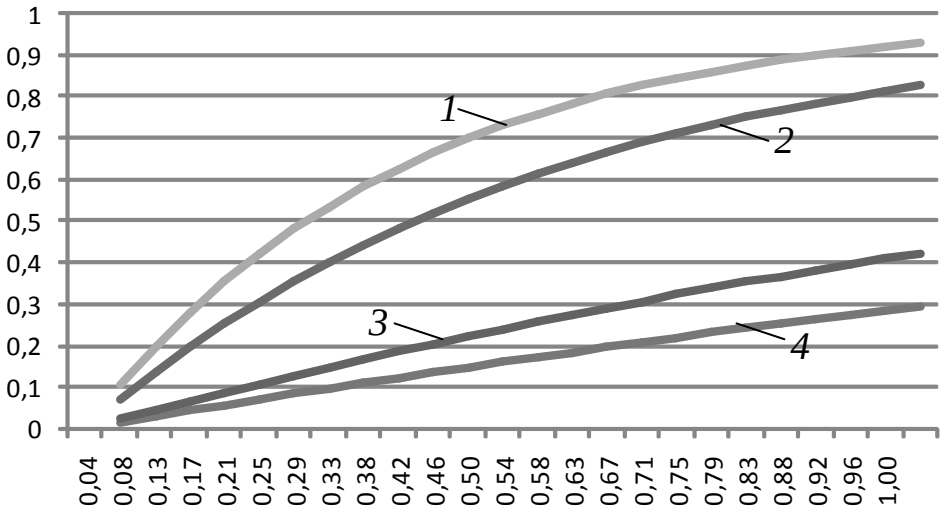


Рисунок 4.3 – Зависимость реализации атак от времени: 1 – *VIA*, 2 – *HSS*, 3 – *FSM*, 4 – *FAS*

Отношение инициализации сценария угрозой соответствует представленным термам в разделе 3.

На основе полученных значений параметров, проводится интегральная оценка вероятности осуществления сценария. Блок оценки сценария представляет собой одноуровневую структуру, и, соответственно, для него необходимо одно множество нечетких мер, зависящее от количества входных параметров. Учитывая, что сценарии между собой не взаимодействуют, для всех блоков нечеткая мера состоит из 16 элементов множества. Однотипность структуры сценариев позволила определить для всех сценариев одинаковую меру

$$FAS, FSM, VIA, HSS = [0,\ 0.01,\ 0.44,\ 0.13,\ 0.89,\ 0.17,\ 0.36,\ 0.24,\ 0.44,\ 0.63,\ 0.68,\ 0.09,\ 0.26,\ 0.79,\ 0.23,\ 1]$$

Входные параметры для оценки риска следующие: $PT(T)$ – получены в результате оценки угрозы; $PTS(TS)$ – получены в результате моделирования сценариев; $YTS(TS)$ – определяется на основе соответствующих факторов угроз

$$YTS(FAS) = [0.33, 0.63, 0.95, 0.21, 0.47, 0.36, 0.14, 0.1]$$
$$YTS(FSM) = [0.54, 0.41, 0.26, 0.94, 0.27, 0.57, 0.9, 0.05]$$
$$YTS(VIA) = [0.28, 0.41, 0.26, 0.94, 0.27, 0.57, 0.9, 0.81]$$
$$YTS(HSS) = [0.12, 0.41, 0.26, 0.94, 0.27, 0.57, 0.9, 0.41]$$

Таким образом, основываясь на расчетах с использованием нечеткого интеграла, можно рассчитать оценку каждого сценария

$$PTS(FAS) = [0.79, 0.11, 0.3, 0.82, 0.4, 0.59, 0.15, 0.64, 0.92, 0.56],$$
$$PTS(FSM) = [0.43, 0.59, 0.7, 0.64, 0.99, 0.82, 0.64, 0.76, 0.6, 0.97],$$
$$PTS(VIA) = [0.69, 0.99, 0.36, 0.05, 0.06, 0.4, 0.93, 0.29, 0.03, 0.95],$$
$$PTS(HSS) = [0.47, 0.01, 0.22, 0.35, 0.55, 0.74, 0.31, 0.23, 0.24, 0.88]$$

4.3.4 Оценка возможности возникновения инцидентов безопасности

Каждый из выбранных инцидентов подчиняется различной модели инцидентов, определенных в разделе 2:

– инцидент VBW описывается одиночной моделью $VIA \xrightarrow{C_{Lt}} VBW$;

– инцидент HAR описывается параллельной моделью $\{FAS, FSM\} \xrightarrow{C_{Lt}} HAR$;

– инцидент HAS описывается смешанной моделью $\{\{HSS\}, \{HAR\}\} \xrightarrow{C_{Lt}} HAS$.

В соответствии с выбранными моделями, входными данными для оценки инцидентов являются:

– для инцидента VBW оценка сценария, отношение следствия, оценка уязвимостей, вероятность возникновения инцидента;

– для инцидента HAR две оценки сценариев, отношения влияния от двух сценариев, оценка уязвимостей, вероятность возникновения инцидента;

– для сценария HAS оценка сценария, оценка инцидента, отношения следствия от сценария и инцидента, оценка уязвимостей, вероятность возникновения инцидента.

Вероятность возникновения инцидента безопасности зависит непосредственно от реализации сценария нарушения, и определяется по формуле

$$PUI(UI) = 1 - e^{-3P(TS)}$$

что позволяет определить зависимость вероятности возникновения инцидента от времени протекания сценария.

Соответствующая зависимость возникновения инцидента представлена графиком на рисунке 4.4.

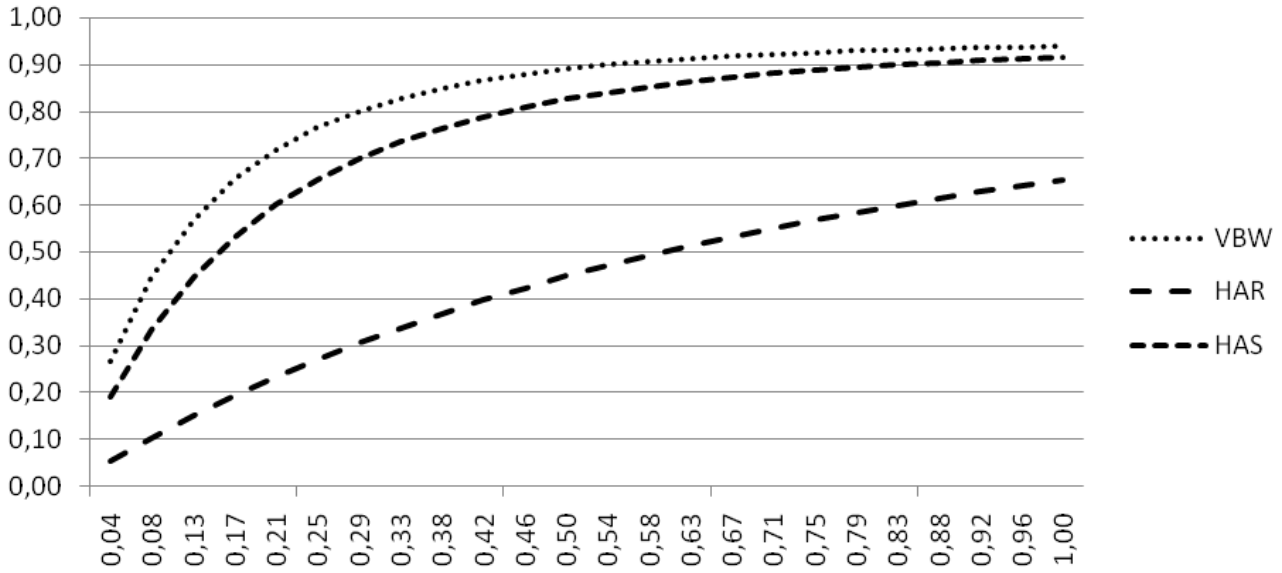


Рисунок 4.4 – Зависимость вероятности возникновения инцидентов от времени осуществления сценария

Лингвистические термы переменной, описывающей отношения следствия, определены в раздел 2. Оценка уязвимостей используется из моделей соответствующих инциденту сценариев.

В соответствии с выявленным количеством параметров для инцидентов, определены следующие нечеткие меры:

VBW = [0, 0.45, 0.49, 0.03, 0.78, 0.11, 0.37, 0.63, 0.66, 0.05, 0.16, 0.97, 0.56, 0.27, 0.31, 1],

HAR = [0, 0.71, 0.61, 0.0, 0.5, 0.62, 0.7, 0.82, 0.99, 0.85, 0.29, 0.02, 0.98, 0.88, 0.8, 0.74, 0.48, 0.56, 0.02, 0.24, 0.93, 0.23, 0.1, 0.14, 1],

HAS = [0, 0.33, 0.48, 0.68, 0.99, 0.41, 0.44, 0.37, 0.67, 0.46, 0.26, 0.8, 0.34, 0.05, 0.66, 1].

Оценка инцидента, возникшего в результате деятельности вируса, определяется следующей моделью

$$PUI(VBW) = F_{UI}(PTS(VIA), C_{Lt}, PUI(VBW), YUI(VBW))$$

В соответствии с расчетами нечеткого интеграла по полученным нечетким мерам получаются соответствующие оценки инцидента

$PUI(VBW)$ = [0.315, 0.479, 0.662, 0.055, 0.536, 0.079, 0.945, 0.986, 0.437, 0.795, 0.767, 0.582, 0.866, 0.496, 0.16, 0.649, 0.397, 0.271, 0.107, 0.128, 0.933, 0.853, 0.254, 0.732, 0.933, 0.585, 0.554, 0.568, 0.832, 0.962].

Оценка инцидента, вызванного ошибками администратора сервисов, определена следующей моделью

$$PUI(HAR) = F_{UI}(PTS(FSM), PTS(FAS), C_{Lt}^{FSM}, C_{Lt}^{FAS}, PUI(HAR), YUI(HAR))$$

В соответствии с расчетами нечеткого интеграла по полученным нечетким мерам получаются соответствующие оценки инцидента

$PUI(HAR)$ = [0.42, 0.979, 0.935, 0.029, 0.359, 0.418, 0.406, 0.567, 0.951, 0.908, 0.848, 0.79, 0.795, 0.236, 0.24, 0.597, 0.306, 0.413, 0.349, 0.305, 0.117, 0.548, 0.159, 0.14, 0.414, 0.984, 0.948, 0.823, 0.042, 0.892, 0.474, 0.532, 0.867, 0.271, 0.566, 0.723, 0.06, 0.475, 0.377, 0.034, 0.423, 0.061, 0.572, 0.077, 0.916].

Оценка инцидента, вызванного действиями злоумышленника, определена следующей моделью

$$P(HAS) = F_{UI}(PTS(HSS), PTS(HAR), C_{Lt}^{HSS}, C_{Lt}^{HAR}, PUI(HAS), YUI(HAS))$$

В соответствии с расчетами нечеткого интеграла по полученным нечетким мерам получаются соответствующие оценки инцидента

$PUI(VBW)$ = [0.492, 0.259, 0.294, 0.628, 0.307, 0.168, 0.919, 0.182, 0.041, 0.143, 0.322, 0.801, 0.574, 0.603, 0.46, 0.813, 0.491, 0.061, 0.519, 0.604, 0.175,

0.641, 0.743, 0.212, 0.763, 0.612, 0.634, 0.59, 0.805, 0.727, 0.458, 0.99, 0.306, 0.739, 0.497, 0.565, 0.505, 0.064, 0.022, 0.977, 0.8, 0.037, 0.827, 0.591, 0.888].

4.3.5 Идентификация и оценка рисков

На основе полученных элементов следует, что выбранный актив подвержен двум рискам, которые определяются двумя инцидентами, непосредственно воздействующим на актив.

Основываясь на оценках инцидентов и значениях отношений ущерба, производится классификация, с целью оценки уровня рисков. Для этого осуществляется кластеризация данных параметров, начальные данные для которой представлены на рисунке 4.5.

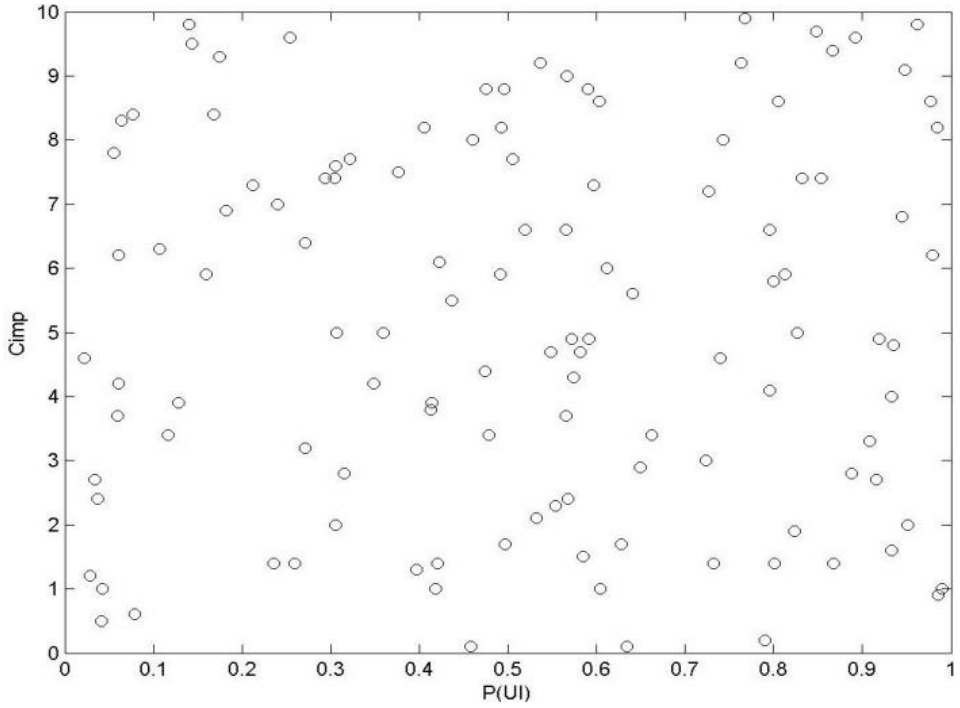


Рисунок 4.5 – Начальные данные для классификации

В полученном пространстве значений производится поиск центров кластеров. Для этого было выбрано 40 кластеров для предварительного анализа группирования значений (рисунок 4.6)

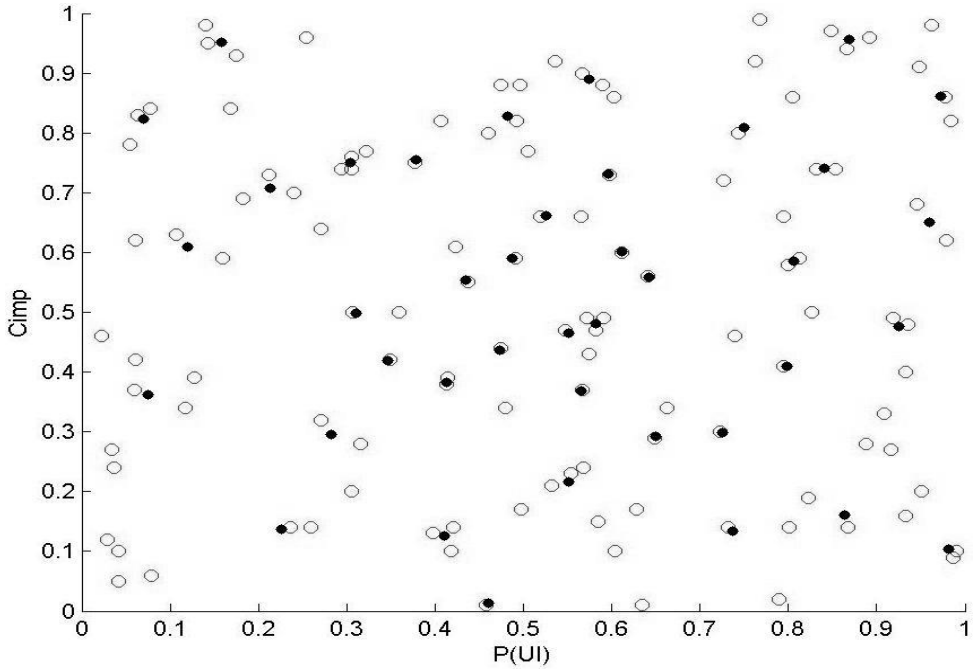


Рисунок 4.6 – Определение центров кластеров

Для дальнейшего объединения кластеров строится матрица, размерность которой равна количеству кластеров, в данном случае 40*40. Путем объединения кластеров с наименьшим расстоянием, получаем пять кластеров, соответствующих количеству термов описания рисков. На основе итоговой кластеризации разработаны правила определения уровня рисков на основе параметров инцидентов и отношений влияния

1. Если $P(UI) < 0{,}365$ & $C_{imp} < 0{,}49$
   то $R =$ "очень низкий"
2. Если $P(UI) < 0{,}365$ & $C_{imp} \geq 0{,}49$ & $C_{imp} < 0{,}67$
   и $P(UI) > 0{,}365$ & $P(UI) < 0{,}43$ & $C_{imp} < 0{,}67$
   и $P(UI) < 0{,}52$ & $P(UI) < 0{,}43$ & $C_{imp} < 0{,}21$
   то $R =$ "низкий"
3. Если $P(UI) < 0{,}495$ & $C_{imp} > 0{,}67$
   и $P(UI) > 0{,}43$ & $P(UI) < 0{,}485$ & $C_{imp} < 0{,}66$ & $C_{imp} > 0{,}21$
   и $P(UI) > 0{,}485$ & $P(UI) < 0{,}815$ & $C_{imp} < 0{,}45$ & $C_{imp} > 0{,}215$

и $P(UI) < 0{,}815$ & $P(UI) > 0{,}52$ & $C_{imp} < 0{,}215$

то $R =$ "средний"

4. Если $P(UI) < 0{,}72$ & $C_{imp} > 0{,}495$ & $C_{imp} > 0{,}45$

и $P(UI) > 0{,}72$ & $C_{imp} > 0{,}455$ & $C_{imp} < 0{,}67$

и $P(UI) > 0{,}815$ & $C_{imp} < 0{,}455$

то $R =$ "высокий"

5. Если $P(UI) > 0{,}72$ & $C_{imp} > 0{,}66$

то $R =$ "очень высокий"

Основываясь на данных кластерах и правил к ним, определяется граница допустимости или недопустимости уровня риска RLA. В общем случае такой границей может выступать линия разграничения кластеров, следовательно, «высокий» и «очень высокий» риски принимаются недопустимыми. Риски «средний», «низкий» и «очень низкий» считаются приемлемыми.

Если R = “очень низкий” то RLA = “допустимый”

Если R = “низкий” то RLA = “допустимый”

Если R = “средний” то RLA = “допустимый”

Если R = “высокий” то RLA = “недопустимый”

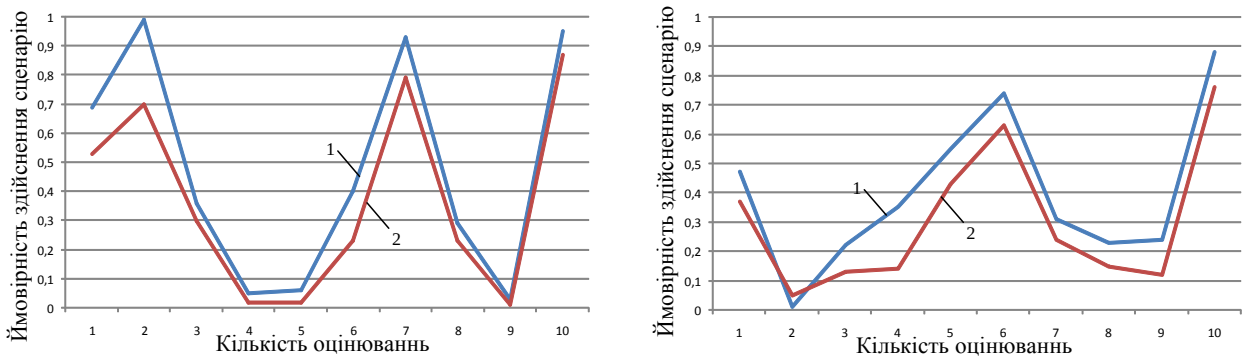
Если R = “очень высокий” то RLA = “недопустимый”

В соответствии с полученными уровнями рисков и их допустимости можно осуществлять мероприятия по обработке риска.

4.4 Результаты анализа рисков

В ходе экспериментальных исследований были получены промежуточные и итоговые оценки процессов нарушения безопасности информационной системы, которые возможно сравнить с известными методами.

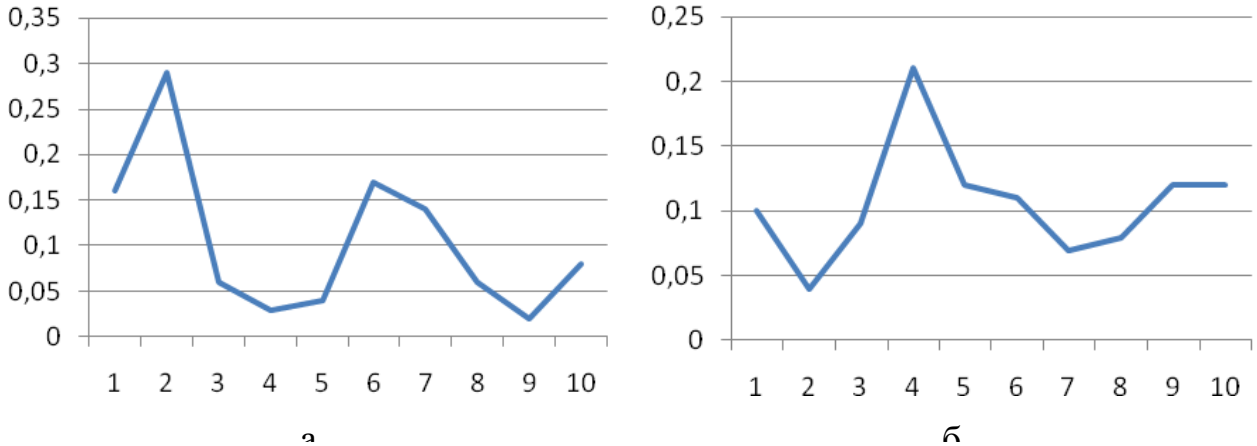
Метод оценки угроз позволил повысить адекватность определения источников нарушения безопасности, что, в свою очередь, позволило повысить качество моделирования процессов нарушения информационной безопасности. Сравнительная характеристика моделирования сценариев с использованием оценки угроз и без нее представлена на рисунке 4.7.



а б

Рисунок 4.7 – Сравнительная характеристика оценки сценариев: а – с использованием оценки угроз; б – без оценки угроз, 1 – сценарий HSS, 2 – сценарий VIA

При этом абсолютное отклонение наблюдалось в ложноотрицательную сторону, и в среднем составило 0.105 (рисунок 4.8).



а б

Рисунок 4.8 – Отклонение между оценками сценариев: а – сценарий *VIA*; б – сценарий *HSS*

Предложенный способ моделирования сценариев нарушения угроз с использованием нечетких параметров позволил повысить точность моделирования за счет применения диапазонных параметров для описания этапов осуществления атаки. Сравнительная характеристика моделирования представлена в таблице 4.2.

Таблица 4.2 – Сравнительная оценка качества моделирования

Сценарний	Авторский метод		Метод Coras		Риск-модели ИТКС	
	MSE	MAPE	MSE	MAPE	MSE	MAPE
HSS	0,002	19,3%	0,022	56,3%	0,008	36,4%
VIA	0,005	16,3%	0,016	47,7%	0,001	42,7%
FAS	0,005	24,7%	0,012	62,6%	0,022	43,8%
FSM	0,004	23,2%	0,013	57,1%	0,024	29,6%
Ср-е	0,004	20,9%	0,016	55,93%	0,016	38,1%

Оценка производилась по двум критериям MSE и MAPE, которые показывают отклонение значения модели от наблюдений. Согласно данным критериям, моделирование с нечетко заданными параметрами повышает качество моделей в среднем на 38 %, что в свою очередь позволяет в дальнейшем более адекватно оценить возникновение инцидентов безопасности в информационной системе.

При оценке адекватности классификационных решений об уровне рисков были использованы два множества оценок вероятности инцидентов – оценки в результате нечеткой кластеризации и оценки, основанные на наблюдениях в ходе эксперимента. При этом соответствующие пары оценок учитывались в паре с идентичными значениями отношения вреда. При этом оценки, полученные при наблюдении, использовались как обучающая выборка для анализа, а оценки кластеризации, соответственно, как тестовая выборка. Отклонение оценок инцидентов, полученных в результате моделирования, от экспериментальных представлено на рисунке 4.9.

Полученные в результате кластеризации решения об уровне рисков, сравнивались с экспериментальными наблюдениями реального ущерба, что позволило определить достоверность оценки рисков для каждой из представленных групп.

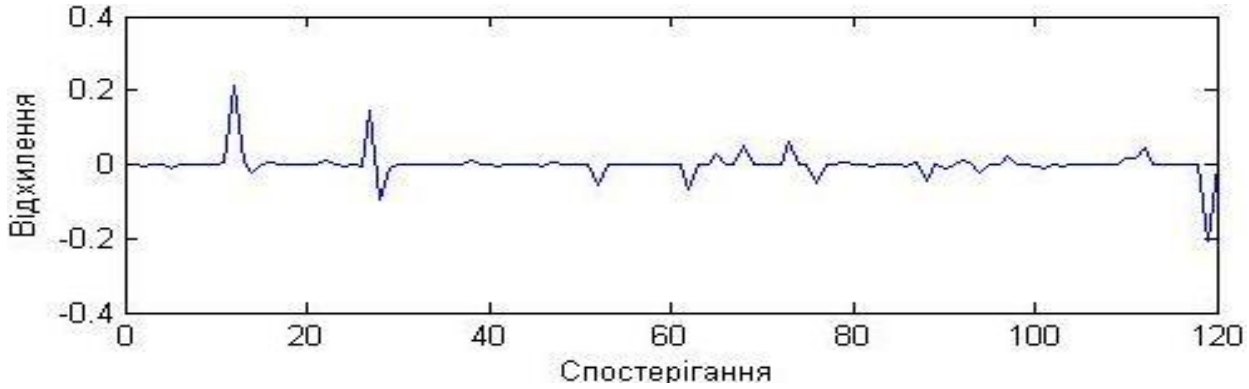


Рисунок 4.9 – Отклонение оценок инцидентов от экспериментальных данных

Распределение оценок рисков полученных в результате кластеризации представлено на рисунке 4.10

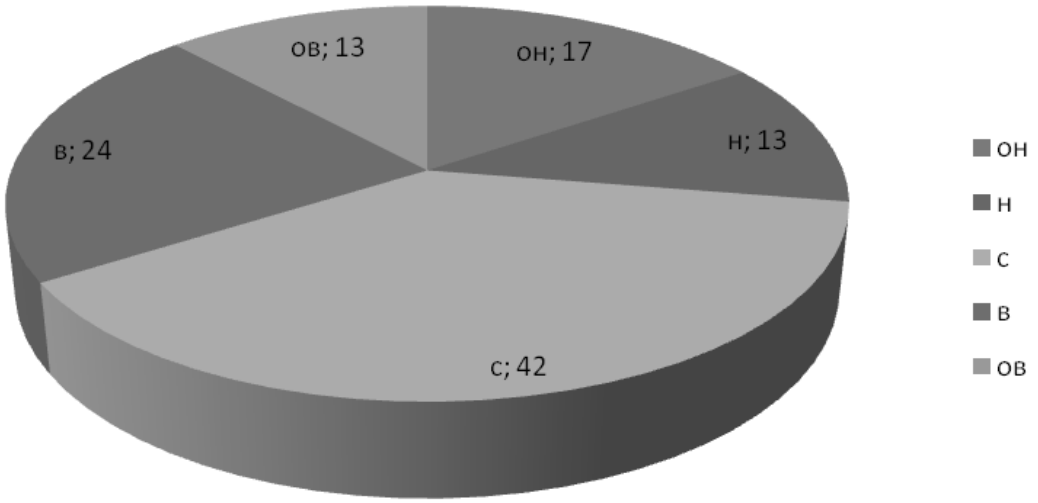


Рисунок 4.10 – Распределение результатов классификации рисков: ОН – «очень низкий»; Н – «низкий»; С – «средний»; В – «высокий»; ОВ – «очень высокий»

При этом было определено, сколько оценок риска при кластеризации совпало с реальной экспериментальной оценкой (рисунок 4.11)

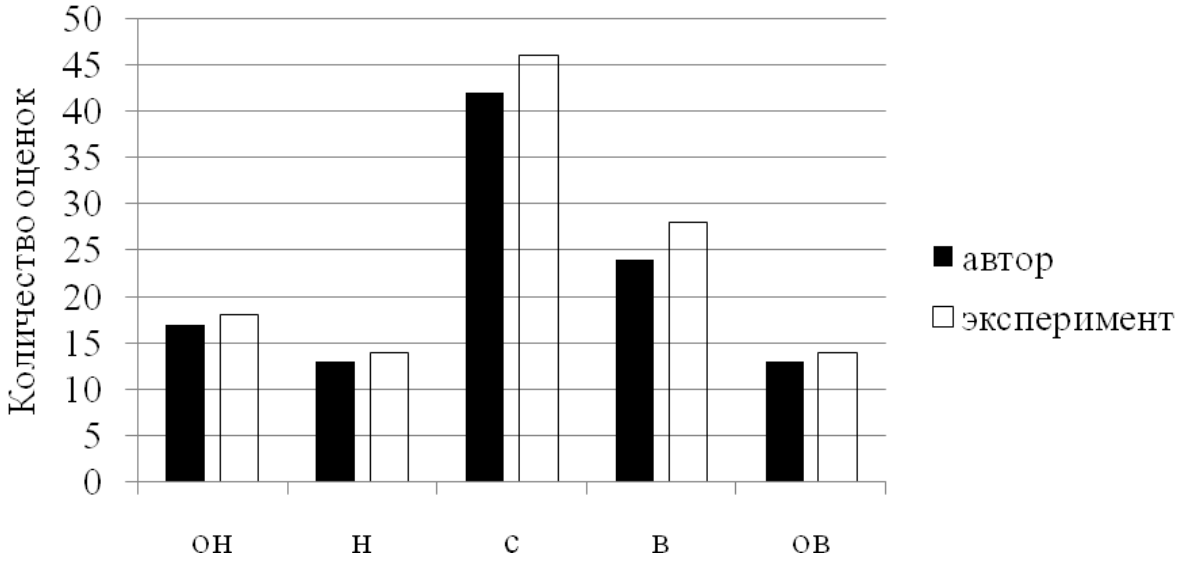


Рисунок 4.11 – Количество правильных оценок риска по отношению к экспериментальным данным

Для оценки достоверности, полученных в результате нечеткой классификации, решениях об уровне риска также были определены значения ошибок первого и второго рода при осуществлении оценок. На основе всех этих данных были получены следующие значения (таблица 4.3).

Таблица 4.3 – Характеристика решений об уровне риска

Уровень	ИТ	Coras	ИТКС	Эксп-т	$D_{ИТ}$	D_{Coras}	$D_{ИТКС}$
1:он	17	16	17	17	1	0.94	1
2:н	14	13	13	15	0.93	0.87	0.87
3:с	39	29	37	41	0.95	0.71	0.90
4:в	31	24	28	33	0.94	0.73	0.85
5:ов	14	11	13	14	1	0.79	93
	Σ=115	*Σ=93*	*Σ=108*	*Σ=120*	$\mu = 0.96$	$\mu = 0.80$	$\mu = 0.93$

D_i – достоверность соответствующего метода по уровням риска, μ – среднее значение достоверности

Исходя из полученных данных видно, что достоверность решения об уровне рисков с использованием разработанной информационной технологии составляет 0.96, при средней вероятности ложноотрицательной ошибки (2-го

рода) 0.025. Также результаты разработанной технологии были сравнены с результатами популярных современных методов.

Таблица 4.4 – Сравнение оценок уровня риска с другими методами

Уровень риска	Информационная технология	Coras	Риск-моделі ИТКС
Достоверность			
дн	1	0.94	1
н	0.93	0.87	0.87
с	0.95	0.71	0.90
в	0.94	0.73	0.85
дв	1	0.79	0.93
Среднее	0.96	0.81	0.91
Вероятность ошибки первого рода			
	$\alpha = 0.017$	$\alpha = 0.067$	$\alpha = 0.033$
Вероятность ошибки второго рода			
	$\beta = 0.025$	$\beta = 0.158$	$\beta = 0.067$

Учитывая тот факт, что подходы к оценке рисков в достаточной мере отличается, сравнение результатов осуществлялась на основе итогового решения об уровне рисков.

Сравнение результатов оценки рисков показало, что достоверность оценки с использованием разработанной информационной технологии в среднем составляет 0.96, что лучше в среднем на 5% при решении о приемлемом уровне риска и на 8% при решении о неприемлемый уровне риска чем с использованием известных методов. Количество ошибок второго рода составило 2,5%, что в среднем лучше на 4,2% чем в математических методах и до 13% чем в статистических методах.

4.5 Выводы

В данном разделе была разработана информационная технология анализа рисков, разработан программно-инструментальный комплекс анализа рисков и проведены экспериментальные исследования методов анализа рисков:

– определены основные этапы и их последовательность для осуществления процесса анализа рисков с применением разработанных методов и моделей;

– разработан программно-инструментальный комплекс, реализующий разработанную информационную технологию. В данном комплексе представлены структуры, позволяющие автоматизировать моделирование процессов нарушения безопасности системы и анализировать полученные данные;

– проведена оценка адекватности разработанных моделей и достоверности полученных результатов. Показано, что применение подходов, основанных на использовании элементов нечеткой логики, дают большую достоверность анализа и оценки рисков, при схожих начальных условиях.

ВЫВОДЫ

В диссертационной работе решена научно-техническую задачу, которая заключается в разработке моделей и методов анализа рисков безопасности информационных систем на основе применения и совершенствования моделей с нечеткими параметрами, а также использовании нечеткого интеграла для агрегации параметров моделей и нечетких баз знаний для оценки уровня рисков.

1. Проведен анализ особенностей угроз информационной безопасности и методов анализа и оценки рисков. Это позволило выделить основные этапы выявления объектов и процессов нарушения информационной безопасности с последующей оценкой рисков нанесения ущерба активов.

2. Разработан метод лингвистической оценки активов информационной системы. Использование данного метода позволило оценивать свойства активов как в качественном формате, так и в количественном формате. Это позволяет проводить оценку не только экспертами, но и менее квалифицированными участниками анализа, позволяет минимизировать количество экспертов.

3. Разработка и использование моделей сценариев нечеткими параметрами позволили повысить точность моделирования сценариев нарушения безопасности. В ходе экспериментальных исследований в работе было обнаружено, что использование данных моделей улучшило определения вероятности реализации сценариев угроз в системе на 7 - 17% в зависимости от типа сценария.

4. Разработанный метод оценки вероятности возникновения угроз позволил структурировать факторы влияния на возникновение факторов событий безопасности. Экспериментально доказано, что данный метод позволяет оценивать возможность возникновения угрозы на основе множества факторов влияния с достоверностью 0.9, что на 8% лучше чем известные методы.

5. Использование нечеткого интеграла и коэффициентов, основанных на нечеткой мере, позволило повысить точность оценки вероятностей возникновения угроз и инцидентов, и вероятность реализации сценариев угроз.

6. Разработанный в работе метод лингвистической оценки рисков с использованием нечеткой кластеризации значений инцидентов и ущерба от них позволил выявлять низкие и высокие уровни рисков с достоверностью 0.97 и 0.96 соответственно, что лучше известных методов на 5 - 8%.

7. Разработана информационная технология анализа рисков безопасности информационных систем, которая позволяет автоматизировать основные этапы оценки элементов рисков и снизить количество участников процесса анализа. Использование данной информационной технологии позволило оценивать уровни рисков со средней достоверностью 0.96 с вероятностью ошибочного решения 0.025.

8. Внедрение разработанной информационной технологии на ООО «Телекарт-Прибор» (г.. Одесса) позволило повысить достоверность оценки рисков на 7-11%. В ходе дальнейшего периодического мониторинга рисков было потрачено на 23% меньше времени, равный 10 часам, на 13 часов до внедрения информационной технологии.

СПИСОК ЛИТЕРАТУРЫ

1. Информационные системы: учебное пособие / [Е. В. Бурцева, И. П. Рак, А. В. Селезнев и др.]. – Тамбов: Изд-во Тамб. гос. техн. ун-та, 2009. – 128с.

2. Информационные системы: учебник для вузов. / Ю. С. Избачев, В. Н. Петров, А. А. Васильев, И. С. Телина – СПб.: Питер, 2011. – 544с.

3. Барабанова, М. И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях / М. И. Барабанова, В. И. Кияев – СПб.: Издательство СПбГУЭФ, 2010. – 267с.

4. Олифер, В. Г. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов / В. Г. Олифер, Н. А. Олифер – СПб.: Питер, 2010. – 944с.

5. Клейменов, С. А. Администрирование в информационных системах: учеб. пособие для студентов высших учебных заведений / С. А. Клейменов, В. П. Мельников, А. М. Петраков. – М.: Издательский центр «Академия», 2008. – 272с.

6. Крэйг Хант. TCP/IP. Сетевое администрирование / Крэйг Хант ; [пер. с англ.; 3-е изд.] – СПб.: Символ-Плюс, 2007. – 816с.

7. Рыжова, В. А. Проектирование и исследование комплексных систем безопасности / Рыжова В. А. – СПб.: НИУ ИТМО, 2013. – 156с.

8. Скиба, В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов – СПб.: Питер, 2008. – 320с.

9. Мао Венбо. Современная криптография: теория и практика / Мао Венбо. – М.: Издательский дом «Вильямс», 2005. – 768с.

10. Владимиров, А. А. Wi-фу: «боевые» приемы взлома и защиты беспроводных сетей / А. А. Владимиров, К. В. Гавриленко, А. А. Михайловский. – М.: НТ Пресс, 2005. – 463с.

11. Фленов, М. Е. Компьютер глазами хакера / Фленов М. Е. – СПб.: БХВ-Петербург, 2005. – 336с.

12. Платонов, В. В. Программно-аппаратные средства защиты информации / В. В. Платонов. – М.: Издательский центр «Академия», 2013. – 336с.

13. Петр Ташков. Защита компьютера на 100 %: сбои, ошибки и вирусы / Петр Ташков. – СПб.: Питер, 2010. – 288с.

14. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах / В. Ф. Шаньгин. – М.: ИД «ФОРМУМ» : ИНФРА-М, 2010. – 592с.

15. Корячко, В. П. Корпоративные сети: технологии, протоколы, алгоритмы / Корячко В. П., Перепелкин Д. А. – М.: Горячая линия – Телеком, 2011. – 216с.

16. Maria Garnaeva. Kaspersky Security Bulletin 2015. Overall statistics for 2015 / [Maria Garnaeva, Jornt van der Wiel, Denis Markushin and etc.]. - Kaspersky Lab, 2015. – 86p.

17. Безбогов, А. А. Безопасность операционных систем / А. А. Безбогов, А. В. Яковлев, Ю. Ф. Мартемьянов. – М.: «Издательство Машиностроение - 1», 2007. – 220с.

18. Хогланд Грег. Взлом программного обеспечения: анализ и использование кода / Хогланд Грег [пер. с англ.] – М.: Издательский дом «Вильямс», 2005. – 400с.

19. Козиол Джек. Искусство взлома и защиты систем / [Козиол Дж., Личфилд Д., Эйтел Д., Энли К. и др.; пер. с англ.]. – СПб.: Питер, 2006. – 416с.

20. Штовба, С. Д. Проектирование нечетких систем средствами MATLAB / С. Д. Штовба. – М.: Горячая линия – Телеком, 2007. – 288с.

21. Кельтон, В. Имитационное моделирование / В. Кельтон, А. Лоу [пер. с англ.]. – СПб.: Питер, Киев: Издательская группа BHV, 2004. – 847с.

22. Борисов, В. В. Нечеткие модели и сети / В. В. Борисов В. В. Круглов, А. С. Федулов. – М.: Горячая линия – Телеком, 2007. – 284с.

23. Радько, Н. М. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. / Н. М. Радько, И. О. Скобелев. – М.: РадиоСофт, 2010. – 232с.

24. Бодянский, Е. В. Нейро-фаззи сети Петри в задачах моделирования сложных систем / Е. В. Бодянский, Е. И. Кучеренко, А. И. Михалев. – Дніпропетровськ: Системні технології, 2005. – 311с.

25. Болдак, А. А. Определение количества кластеров в статистических данных / А. А. Болдак, Д. Л. Сухарев. – К.: Вісник НТУУ КПІ. Інформатика, управління та обчислювальна техніка . – 2011. – 188-122с .

26. Леоненков, А. В. Нечеткое моделирование в среде MATLAB и fuzzyTECH / А. В. Леоненков. – С б.: БХВ-Петербург, 2005. – 736с.

27. Рудниченко, Н. Д.. Нечетко-вероятностная модель оценок рисков сложных технических систем / Н. Д. Рудниченко, В. В. Вычужанин // Інформатика та математичні методи в моделюванні, 2014. Том 4, №3. – 225-232сс.

28. Ехлаков, Ю. П. Нечеткая модель оценки рисков продвижения программных продуктов / Ю. П. Ехлаков // Бизнес-информатика №3 (29), 2014. – 69-78сс.

29. Гладыш, С. В. Представление знаний об управлении инцидентами информационной безопасности посредством нечетких временных раскрашенных сетей Петри / С. В. Гладыш // Міжнародний науково-технічний журнал «Інформаційні технології та комп'ютерна інженерія» №1 (17), 2010. – 57-64сс.

30. Шаньгин, В. Ф. Защита информации в компьютерных системах и сетях / В. Ф. Шаньгин – М.:ДМК Пресс, 2012. – 592с.

31. Безштанько, В. М. Диофантов метод определения частости нанесения ущерба вследствие реализации угрозы информационной безопасности / В. М. Безштанько, В. В. Цуркан. – Захист інформації, том 15, №4, жовтень-грудень 2013. – 278-283сс.

32. Прогнозирование временных рядов: нечеткие модели / [Т. В. Афанасьева и др.]; под науч. ред. Н. Г. Ярушкиной. – Ульяновск: УлГТУ, 2014. – 145с.

33. Мохор, В. В.. Количественная оценка рисков безопасности информации на основе пробит-анализа / В. В. Мохор, В. В. Цуркан. Реєстрація, зберігання і обробка даних. Методи захисту інформації в комп'ютерних системах і мережах, 2010 Том 12, №3. – 85-92сс.

34. Бычков, Е. Д.. Математические модели управления состояниями цифровой телекоммуникационной сети с использованием теории нечетких множеств / Е. Д. Бычков. – Омск: ОмГТУ, 2010. – 236с.

35. A review of methods for capacity identification in Choquet integral based multi-attribute utility theory: Applications of the Kappalab R package / Michel Grabisch, Ivan Kojadinovic, Patrick Meyer. – Elsevier: European Journal of Operational Research, 2008, 186 (2), pp.766-785.

36. Миронова, В. Г. Сети Петри–Маркова как инструмент создания налитических моделей для основных видов несанкционированного доступа в информационной системе / В. Г. Миронова, А. А. Шелупанов, М. А. Сопов // Доклады ТУСУРа № 1 (25), часть 2. – 2012. — С. 20–24.

37. Lund, M. S. Model-Driven Risk Analysis / M. S. Lund, B. Solhaug, K. Stolen. – Berlin: Springer-Verlag, 2011. – P. 55–62.

38. Zadeh, L. A. Toward a theory of fuzzy information granulation and its centrality in human reasoning and fuzzy logic / L. A. Zadeh // Fuzzy Sets and Systems. – 1997. – Vol. 90, Issue 2. – P. 111–127.

39. Ажмухамедов, И. М. Моделирование на основе экспертных суждений процесса оценки информационной безопасности / И. М. Ажмухамедов // Вестник АГТУ. Сер. Управление, вычислительная техника и информатика. – 2009. – № 2. – С. 101–109.

40. Nieto-Morote, A. A fuzzy approach to construction project risk assessment / A. Nieto-Morote, F. Ruz-Vila. – International Journal of Project Management. – 2011. – Vol. 29, Issue 2. – P. 220–231.

41. Ажмухамедов, И. М. Решение задач обеспечения информационной безопасности на основе системного анализа и нечеткого когнитивного моделирования: монография / И. М. Ажмухамедов. – Астрахань, 2012. – 344 с.

42. Lee A. Kadel. Designing and implementing an effective information security program: protecting the data assets of individuals, small and large businesses / Lee A. Kadel. – Genoa Cite, Wisconsin: SANS Institute, 2004. – 43р.

43. Яцало, Б. И. Система многокритериального анализа решений DecernsMCDA и ее практическое применение / Б. И. Яцало, С. В. Грицюк, В. И. Диденко, О. А. Мирзеабасов / Международный научно-практический журнал «Программные продукты и системы» №2 (106). Тверь, 2014. – 73-84сс.

44. Шнайер, Б.. Секреты и ложь. Безопасность данных в цифровом мире / Б. Шнайер. – Спб.: Питер, 2003. – 368с.

45. Muhai Li. DDoS attaks detection model and its application / Muhai Li, Ming Li, Xiuying Jiang. – WSEAS TRANSACTIONS on COMPUTERS, Issue 8, vol. 7, 2008. – 1159-1168pp.

46. Гатчин, Ю. А. Теория информационной безопасности и методология защиты информации / Ю. А. Гатчин, В. В. Сухостат. — СПб.: СПбГУ ИТМО, 2010. — 98 с.

47. Богданов, В. В. Система обнаружения компьютерных атак на основе положений политики безопасности / В. В. Богданов, Н. И. Синадский / Доклады ТУСУРа № 2 (16), – 2012. – 11-14сс.

48. Домарев, В. В. Безопасность информационных технологий. Методология создания систем защиты / Домарев В. В. – К.: "ТИД "ДС", 2002 – 688 с.

49. ГОСТ Р 51901.13-2005. Менеджмент риска. Анализ дерева неисправностей. – Введ. 2005.31.05. – М.: Изд-во стандартов, 2005. – 11с.

50. ГОСТ Р ИСО/МЭК 31010 – 2011. Менеджмент риска. Методы оценки риска. – Введ. 2011.01.12. – М.: Стандартинформ, 2012. – 69с.

51. Шапорин, В. О.Метод расчета размеров буферов коммутаторов / Шапорин Р. О., Шапорин В. О., Милейко И. Г. //Труды Одесского политехнического университета, № 2(28), 2007 – С. 116-118.

52. Шапорин, В.О.Влияние широковещательного и служебного трафика на пропускную способность корпоративной компьютерной сети / Шапорин Р. О., Шапорин В. О. // Електромашинобудування та електрообладнання, № 72, 2009 – С. 113-115.

53. Оценка вероятности проведения атаки на сетевые ресурсы с использованием аппарата нечеткой логики / В. О. Шапорин, П. М. Тишин, Н. Б. Копыт-

чук, Р. О. Шапорин // Електротехнічні та комп’ютерні системи. – К.: Техника. – 2013.– № 12 (88). – С. 95 – 101.

54. Шапорин, В. О. Лингвистическая оценка активов сложной компьютерной системы для анализа рисков информационной безопасности / В. О. Шапорин, П. М. Тишин, Р. О. Шапорин // Електротехнічні та комп’ютерні системи. – К.: Техника. – 2015.– № 18 (94). – С. 28 – 32.

55. Шапорин, В. О. Разработка моделей угроз информационной безопасности для оценки вреда активам / Шапорин В. О., Плачинда О. Е. // Технологический аудит и резервы производства. – 2015. – Том 4 №2 (24). – С. 10-15.

56. Разработка лингвистической модели оценки рисков активов информационной системы / Шапорин В. О., Тишин П. М., Шапорин Р. О., Копитчук Н. Б. // Восточно-Европейский журнал передовых технологий. – 2015. том 4 №2 (76). – С.30-35.

57. Шапорин, В. О. Метод проектирования коммуникационной системы компьютерной сети масштаба предприятия / Шапорин Р.О., Шапорин В.О., Фомина А.А. // Тез. доп. 8-ї міжнар. конф. CIET, 2007 – с. 135.

58. Шапорин, В. О. Аналіз проблем маршрутизації в mesh-мережах / Шапорін Р. О., Шапорін В. О., Кобилянська О. Л. // Тез.доп. 12-ї міжнародної науково-практичної конференції CIET, 2011 – С.139.

59. Нечеткие лингвистические модели обеспечения безопасности компьютерных сетей / Шапорин В. О., Тишин П. М., Копытчук Н. Б., Шапорин Р. О. // Тез.доп. 14-ї міжнародної науково-практичної конференції CIET, 2013 – с. 155-156.

60. Разработка нечетких лингвистических моделей сетевых атак для анализа рисков в распределенных информационных системах / Шапорин В. О., Тишин П. М., Копытчук Н. Б., Шапорин Р. О. //Тез. доп. 15-ї міжнародної науково-практичної конференції CIET, 2014 – с. 131-132.

61. Шапорин, В. О. Определение прав доступа к удаленной лаборатории / Шапорин В. О., Шапорина Е. Л., Перебейнос И. А.// Тез. доп. 15-ї міжнародної науково-практичної конференції CIET, 2014 – с. 100-101.

62. Шапорин, В. О. Автоматизированная система мониторинга экологической ситуации / Шапорин В. О., Шапорина Е. Л., Желиховская Ю. С. //Тез. доп. 15-ї міжнародної науково-практичної конференції СІЕТ, 2014 – с. 60-61.

63. Шапорин, В. О. Способы обеспечения безопасности компьютерных сетей / Шапорин В. О., Шапорина Е. Л., Кощей А. Д. //Тез. доп. 15-ї міжнародної науково-практичної конференції СІЕТ, 2014 – с. 141-142.

64. Шапорин, В. О. Факторы влияния на возникновение угроз безопасности информационной системы / Шапорин В. О. Бабий А. А. // Мат. сем. "Моделювання в прикладних наукових дослідженнях",– 2015. – Вип. XXIII. - с. 77-78.

65. Ахаев, А. В. Метод выбора програмного продукта на основе интеграла Шоке и империалистического алгоритма / А. В. Ахаев, И. А. Ходашинский, А. Е. Анфилосьев / Доклады ТУСУРа № 2 (32), – 2014. – 224-229сс.

66. Птускин, А. С. Модель выбора антирисковых стратегических программ для уменьшения потерь в цепах поставок с нечеткими параметрами / А. С. Птускин // Стратегии бизнеса №2 (2), 2013. – 61- 65сс.

67. Сакулин, С. А.. К вопросу о практическом применении нечетких мер и интеграла Шоке / С. А. Сакулин, А. Н. Алфимцев // Вестник МГТУ им. Н.Э. Баумана. Сер. “Приборостроение”, 2012. – 55-63сс.

68. Лысенко, Ю. Г.. Нечеткая модель эффективности подсистемы нормирования информационной системы управления промышленного предприятия / Ю. Г. Лысенко, Е. Е. Бизянов // Міжнародний науковий журнал «Економічна кібернетика» №1-3 (73-75), 2012. – 16-25сс.

69. Силов, В. Б.. Принятие стратегических решений в нечеткой обстановке / В. Б. Силов. – М.: ИНПРО – РЕС, 1995. – 228с.

70. Рыжов, А. П. Об агрегировании информации в нечетких иерархических системах / Рыжов А. П // Интеллектуальные системы, Том 6, вып. 1-4, Москва, 2001. – 23с.

71. Ватковский, С. А.. Нечеткие модели марковских процессов в теории надежности / С. А. Ватковский, Т. Г. Емельяненко // Актуальні проблеми авто-

матизації та інформаційних технологій, Том 16, Дніпропетровськ, 2012. – 18-28сс.

72. Бочарников, В. П. Fuzzy-технология: Математические основы. Практика моделирования в экономике. – СПб.: «Наука» РАН, 2001. – 328с.

73. Батыршин, И. З.. Основные операции нечеткой логики и их обобщения / И. З. Батыршин. – Казань: Отечество, 2001. – 100с.

74. Птускин, А. С.. Нечеткие модели и методы в менеджменте / А. С. Птускин. – М: Издательство МГТУ им. Н. Э. Баумана, 2008. – 11с.

75. Недашківська, Н. І. Багатокритеріальне оцінювання альтернатив при взаємозалежних критеріях за допомогою методу BOCR/MAI та нечітких мір / Н. І. Недашківська. – Системи підтримки прийняття рішень. Теорія і практика, Київ, 2011. – 71-75сс.

76. Крылов, С. М. Онтология проектирования гетерогенних электронных систем / Крылов С. М., Гребенщиков Е. Н. // Научный журнал «Онтология проектирования», № 1 (3), 2012. – 65-72сс.

77. Сакулин, С. А.. Операторы агрегирования в нечетких диагностических моделях технологических процессов производств протяженных изделий / С. А. Сакулин // Вестник ТГТУ. Том 13, № 1А, 2007. – 57-70сс.

78. Павлов, А. Н.. Принятие решений в условиях нечеткой информации: учебное пособие /А. Н. Павлов, Б. В. Соколов. – СПб.: ГУАП, 2006. – 72с.

79. Холзнер, С. XML. Энциклопедия / Холзнер С. – СПб.: Питер, 2004. – 1101с.

80. Гарольд, Э. XML. Справочник / Гарольд Э., Минс С. – СПб.: Символ-Плюс, 2002. – 576с.

81. Лотфи Заде. Понятие лингвистической переменной и его применение к принятию приближенных вычислений / Л. Заде. – пер. с англ. Н. И. Ринго. – М.: Издательство «МИР», 1976. – 165с.

82. Подиновский, В. В. Парето-оптимальные решения многокритериальных задач / Подиновский В. В., Ногин В. Д. – М.:ФИЗМАТЛИТ, 2007. – 256с.

83. Поляк, Б. Т. Введение в оптимизацию / Поляк Б. Т. – М.: Наука. Главная редакция физико-математической литературы, 1983. – 384с.

84. Блюмин, С. Л.. Применение нечетких мер и интегралов к описанию нечетких динамических систем / С. Л. Блюмин, А. М. Шмырин. – Control Science №3, 2005. – 20-22сс.

85. Жуковин, В. Е.. Нечеткие многокритериальные модели принятия решений / В. Е. Жуковин. – Тбилиси: МЕЦНИЕРЕБА, 1988. – 71с.

86. Чистяков, А. Д.. Теория нечетких множеств в системе методологического инструментария экономики неопределенностей / А. Д. Чистяков, Н.Д. Елецкий. - Современные проблемы экономики и управления, №2 (02), 2012. – 1-18сс.

87. Шапорина, Е. Л. Алгоритм оптимизации характеристик функционирования компьютерных сетей с нечетко заданными параметрами / Шапорина Е. Л., Тишин П. М., Милейко И. Г., Шапорин Р. О. Инновации в науке / Сб. ст. по материалам XXXVI междунар. науч.- практ. конф. № 8(33). Новосибирск: Изд. «СибАК», 2014 – 36-46сс.

88. Нестеренко, С. А. Процедура оптимізації характеристик функціонування комп’ютерних мереж в умовах нечітко заданих параметрів / Нестеренко С. А., Тішин П. М., Шапоріна О. Л., Мілейко І. Г. // Науковий вісник Чернівецького університету. – 2014. – Т. 5, Вип. 1. – С. 38 – 42.

89. Копитчук, Н. Б. Построение набора эталонов для повышения точности экспертных оценок / Н. Б. Копитчук, П. М. Тишин, И. Н. Копытчук, И. Г. Милейко. – Науковий журнал «ScenceRise» №4/2(9), 2015. – 72-77с.

90. Копытчук, Н. Б. Алгоритм определения аномальных ситуаций для тензометрических систем / Копытчук Н. Б., Тишин П. М., Копытчук И. Н., Милейко И. Г. – Збірник наукових праць. Серія: Механіко-технологічні системи та комплекси.– Х.: НТУ „ХПІ» – 2015р. - №21(1130) , с37-45.

91. Копитчук, И.Н.. Построение аппроксимирующей нечеткой зависимости для определения параметров классификации аномалий / И. Н. Копитчук, Н. Б. Копытчук, П. М. Тишин, И. Г. Милейко // Инновации в науке / Сб. ст. по ма-

териалам XXXVI междунар. науч.- практ. конф. № 8(33). Новосибирск: Изд «СибАК», 2014 –с 14-22.

92. Копытчук, Н. Б. Анализ вычислительных сетей с помощью многоуровневой онтологии оценки рисков с применением методологии Coras / Н. Б. Копытчук, П. М. Тишин, М. В. Цюрупа. – Електротехнічні та комп'ютерні системи. – К.: Техника. – 2013.– № 10 (86). – С. 120 – 126.

93. Копытчук, Н. Б. Применение нечеткой дескрипционной логики при разработке формализованного языка анализа рисков / Н. Б. Копытчук, П. М. Тишин, К. В. Ботнарь, М. В. Цюрупа. – Електротехнічні та комп'ютерні системи. – К.: Техника. – 2011.– № 04 (80). – С. 168 – 176.

94. Заде Л. А. Размытые множества и их применение в распознавании образов и кластер-анализе / Заде Л. А.. – М.: Изд-во «МИР», 1980. – 247с.1

Приложение А

А.1 Акт внедрения информационной технологии

ЗАТВЕРДЖУЮ
Генеральний директор
ВАТ «Телекарт-Прибор»
_____ О. С. Козлов
_____ 2016

АКТ

про впровадження інформаційної технології аналізу ризиків у
ВАТ «Телекарт-Прибор»

м. Одеса

Ми, що нижче підписалися, від ВАТ «Телекарт-Прибор» …, від ОНПУ старший викладач кафедри КІСМ Шапорін В.О., склали цей акт у тому, що інформаційна технологія аналізу ризиків інформаційної безпеки, розроблена старшим викладачем кафедри комп'ютерних інтелектуальних систем та мереж ОНПУ Шапоріним В.О., була використана при розробці інформаційних систем ВАТ «Телекарт-Прибор».

З використанням інформаційної технології аналізу ризиків були оцінені ресурси інформаційної системи

Використання технології дозволило на 14% збільшити достовірність оцінки ризиків інформаційної безпеки та на 23% зменшити час на моніторинг ризиків в системі.

Від ВАТ «Телекарт-Прибор»
Зав. відділом
_____

Від ОНПУ
Старший викладач
Кафедри КІСМ
_____ В.О. Шапорін

А2. Справка о внедрении результатов исследования
в учебный процесс

ЗАТВЕРДЖУЮ
Проректор з науково-педагогічної
та виховної роботи
Одеського національного
політехнічного університету
_____ С.А. Нестеренко
_____ 2016

ДОВІДКА
про впровадження результатів дисертаційної роботи
Шапоріна Володимира Олеговича
«Моделі та методи аналізу ризиків безпеки інформаційних систем»
у навчальному процесі ОНПУ

Довідка видана в тому, що в курсах лекцій по дисциплінах «Комп’ютерні мережі», «Захист інформації в комп’ютерних системах», «Дослідження систем штучного інтелекту», що читаються студентам фаху 6.050102 «Комп’ютерна інженерія» та 8.05010201 «Комп'ютерні системи та мережі» у 7, 8 та 10 семестрах відповідно, використовуються наукові результати, отримані в дисертаційній роботі Шапоріна В.О.

Елементи інформаційної технології аналізу ризиків викладаються у темі «Аудіт безпеки комп’ютерних мереж» дисципліни «Комп’ютерні мережі».

Метод аналізу ризиків інформаційної безпеки викладається у темі «Аналіз ризиків» дисципліни «Захист інформації в комп’ютерних системах».

Моделювання сценаріїв загроз з нечіткими параметрами викладаються у темі «» дисципліни «Дослідження систем штучного інтелекту».

Наукові та практичні результати, що отримані в результаті в дисертаційній роботі Шапоріна В.О., також використовуються у дипломному проектуванні.

Зав. каф. «Комп'ютерні інтелектуальні системи та мережі»,
к.т.н., доц. Шапорін Р.О.

Приложение Б

Диаграммы угроз Coras

Рассматривая влияние угроз на функционирование системы, целесообразно декомпозировать диаграмму угроз по виду угрозы. Таким образом, получается четыре диаграммы – угроза «злоумышленник», угроза «вирус», угроза «пользователь», угроза «администраторы». Угроза «злоумышленник» представлена в п.2.1 основной части работы.

Влияние вирусов на активы системы представлено на рисунке Б.1

Описание процессов диаграммы. Вирус является дополнительным источником нарушения работоспособности системы для злоумышленников. Он инициирует сценарии, которые заключаются в инфицировании программных подсистем ИС. Такими подсистемами выступают серверы, сервисы, компьютеры пользователей и другие сетевые устройства (дисковые массивы, контроллеры и т. п.), которые имеют важность для бизнес-процессов организации.

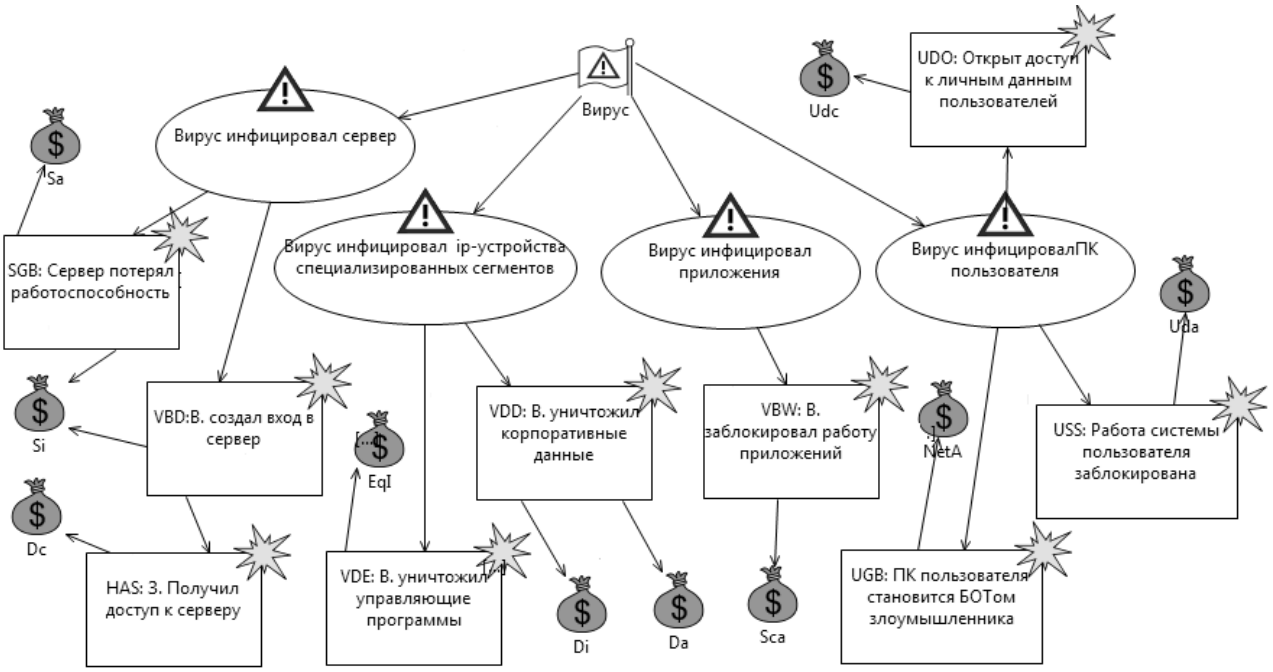


Рисунок Б.1 – Диаграмма угроз. Влияние вируса

Реализация данных сценариев влечет за собой такие нежелательные инциденты, как создание скрытых входов (backdoor) в сеть или системы организа-

ции, открытие личных и корпоративных данных и, что зачастую наиболее критично, уничтожение данных или управляющих программ.

В данной диаграмме используются следующие обозначения:

Угрозы: V – вирус.

Подмножество сценариев угроз: VIS – вирус инфицировал сервер; VID – вирус инфицировал узловые устройства сегментов;VIA – вирус инфицировал приложения;VIP – вирус инфицировал устройства пользователей.

Подмножество нежелательных инцидентов: VBD – создание скрытого входа в серверную системы, предшествует получению прав доступа злоумышленником; VDE – уничтожение вирусом различных управляющих программ, таких как драйверы, СУБД и т. п.; VDD – уничтожение вирусом корпоративных данных, которые находятся на различных носителях; VBW – блокировка работы приложений вирусом, и, как следствие, недоступность сервисов системы; UDO – дискредитация личных данных вирусом; SGB – Сервер потерял работоспособность.

Отношения между данными элементами следующие:

Отношения инициализации сценариев угроз вирусом: $V \xrightarrow{C_{init}(V,VIS)} VIS$ – угроза V инициирует сценарий VIS, при этом переменная $C_{init}(V,VIS)$ описывает вероятность инициализации сценария; $V \xrightarrow{C_{init}(V,VID)} VID$ угроза V инициирует сценарий VID, при этом переменная $C_{init}(V,VID)$ описывает вероятность инициализации сценария; $V \xrightarrow{C_{init}(V,VIA)} VIA$ угроза V инициирует сценарий VIA, при этом переменная $C_{init}(V,VIA)$ описывает вероятность инициализации сценария; $V \xrightarrow{C_{init}(V,VIP)} VIP$ угроза V инициирует сценарий VIP, при этом переменная $C_{init}(V,VIP)$ описывает вероятность инициализации сценария.

Отношения наследия, описывающие возникновение нежелательных инцидентов в результате реализации сценария угроз:$VIS \xrightarrow{C_{Lt}(VIS,SGB)} SGB$ нежелательный инцидент SGB возник в результате выполнения сценария VIS, при этом переменная $C_{Lt}(VIS,SGB)$ описывает вероятность возникновения нежелатель-

ного инцидента; $VIS \xrightarrow{C_{Lt}(VIS,VBD)} VBD$ нежелательный инцидент VBD возник в результате выполнения сценария VIS, при этом переменная $C_{Lt}(VIS, VBD)$ описывает вероятность возникновения нежелательного инцидента; $VID \xrightarrow{C_{Lt}(VID,VDE)} VDE$ нежелательный инцидент VDE возник в результате выполнения сценария VID, при этом переменная $C_{Lt}(VID, VDE)$ описывает вероятность возникновения нежелательного инцидента; $VID \xrightarrow{C_{Lt}(VID,VDD)} VDD$ нежелательный инцидент VDD возник врезультате выполнения сценария VID, при этом переменная $C_{Lt}(VID, VDD)$ описывает вероятность возникновения нежелательного инцидента; $VIA \xrightarrow{C_{Lt}(VIA,VBW)} VBW$ нежелательный инцидент VBW возник в результате выполнения сценария VIA, при этом переменная $C_{Lt}(VIA, VBW)$ описывает вероятность возникновения нежелательного инцидента; $VIP \xrightarrow{C_{Lt}(VIP,UDO)} UDO$ нежелательный инцидент UDO возник в результате выполнения сценария VIP, при этом переменная $C_{Lt}(VIP, UDO)$ описывает вероятность возникновения нежелательного инцидента; $VIP \xrightarrow{C_{Lt}(VIP,USS)} USS$ нежелательный инцидент USS возник в результате выполнения сценария VIP, при этом переменная $C_{Lt}(VIP, USS)$ описывает вероятность возникновения нежелательного инцидента; $VIP \xrightarrow{C_{Lt}(VIP,UGB)} UGB$ нежелательный инцидент UGB возник врезультате выполнения сценария VIP, при этом переменная $C_{Lt}(VIP, UGB)$ описывает вероятность возникновения нежелательного инцидента.

Отношения наследия между нежелательными инцидентами: $VBD \xrightarrow{C_{Lt}(VBD,HAS)} HAS$нежелательный инцидент UGB вызван нежелательным инцидентом VBD, при этом переменная $C_{Lt}(VBD, HAS)$ описывает вероятность возникновения нежелательного инцидента.

Отношения влияния нежелательных инцидентов на активы системы: $SGB \xrightarrow{C_{Lt}(SGB,Sa)} Sa$ нежелательный инцидент SGB привел к снижению оценки актива Sa, при этом переменная $C_{Lt}(SGB, Sa)$ описывает степень влияния инци-

дента на актив; $SGB \xrightarrow{C_{Lt}(SGB,Si)} Si$ нежелательный инцидент SGB привел к снижению оценки актива Si, при этом переменная $C_{Lt}(SGB, Si)$ описывает степень влияния инцидента на актив; $VBD \xrightarrow{C_{Lt}(VBD,Si)} Si$ нежелательный инцидент VBD привел к снижению оценки актива Si, при этом переменная $C_{Lt}(VBD, Si)$ описывает степень влияния инцидента на актив; $HAS \xrightarrow{C_{Lt}(HAS,Dc)} Dc$ нежелательный инцидент HAS привел к снижениюоценки актива Dc, при этом переменная $C_{Lt}(HAS, Dc)$ описывает степень влияния инцидента на актив; $VDE \xrightarrow{C_{Lt}(VDE,EqI)} EqI$ нежелательный инцидент VDE привел к снижению оценки актива EqI, при этом переменная $C_{Lt}(VDE, EqI)$ описывает степень влияния инцидента на актив; $VDD \xrightarrow{C_{Lt}(VDD,Di)} Di$ нежелательный инцидент VDD привел к снижению оценки актива Di, при этом переменная $C_{Lt}(VDD, Di)$ описывает степень влияния инцидента на актив; $VDD \xrightarrow{C_{Lt}(VDD,Da)} Da$ нежелательный инцидент VDD привел к снижению оценки актива Da, при этом переменная $C_{Lt}(VDD, Da)$ описывает степень влияния инцидента на актив; $VBW \xrightarrow{C_{Lt}(VBW,Sca)} Sca$ нежелательный инцидент VBW привел к снижению оценки актива Sca, при этом переменная $C_{Lt}(VBW, Sca)$ описывает степень влияния инцидента на актив; $UGB \xrightarrow{C_{Lt}(UGB,NetA)} NetA$ нежелательный инцидент UGB привел к снижению оценки актива $NetA$, при этом переменная $C_{Lt}(UGB, NetA)$ описывает степень влияния инцидента на актив; $USS \xrightarrow{C_{Lt}(USS,Uda)} Uda$ нежелательный инцидент USS привел к снижению оценки актива Uda, при этом переменная $C_{Lt}(USS, Uda)$ описывает степень влияния инцидента на актив.

Как указывалось ранее, источником вреда в системе могут быть и ее легальные участники. Влияние на систему ее пользователей представлено на рисунке Б.2.

Описание процессов диаграммы. Все пользовательские сценарии угроз, в основном, связаны с неосторожным обращением с системой и личными данными.

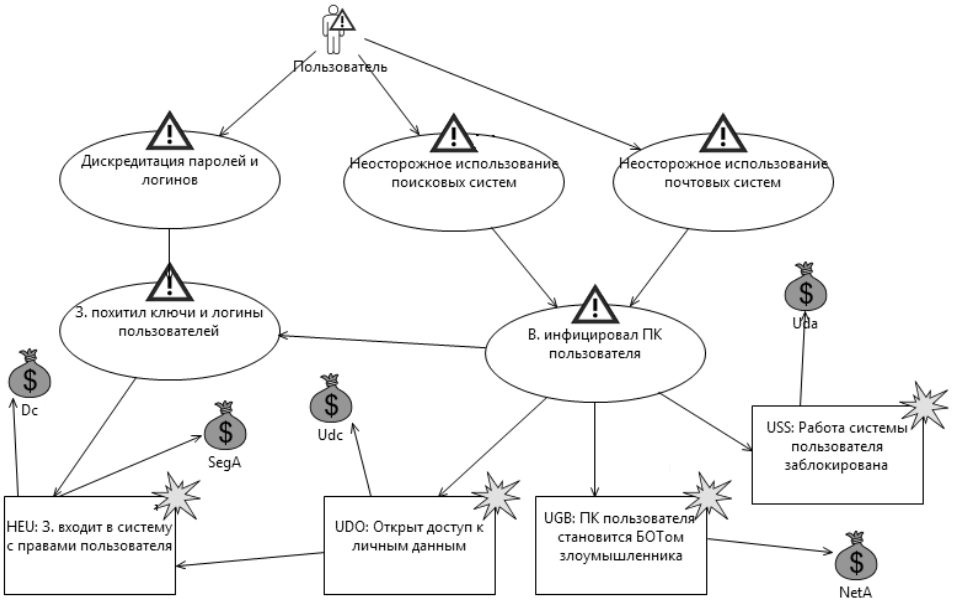


Рисунок Б.2 – Диаграмма угроз. Влияние пользователей

Такими сценариями могут быть дискредитация логинов и паролей, неосторожная или неправильная работа в Inetrnet, в частности с поисковыми и почтовыми системами, что влечет за собой инфицирование вирусами. Данные сценарии влекут за собой нежелательные инциденты, которые, в основном связаны с дальнейшей деятельностью вирусов и злоумышленников.

В данной диаграмме введены следующие обозначения:

Угрозы: U – пользователь.

Подмножество сценариев угроз: DPL – пользователь дискредитировал пароли и логины; HSP – злоумышленник похитил ключи и логины пользователей; FSS – пользователь неосторожно использовал поисковую систему; VIP - вирус инфицировал устройства пользователя; FMS - пользователь неосторожно использовал почтовую систему.

Подмножество нежелательных инцидентов: HEU – В следствие хищения или утери паролей и ключей, злоумышленник получил возможность войти в систему с правами легального пользователя; UGB – в следствии заражения вирусом, устройство пользователя становится управляемым сценариями злоумышленника; USS – система пользователя потеряла работоспособность; UDO – открыт доступ к личным данным пользователей.

Отношения между данными элементами следующие:

Отношения инициализации сценариев угроз пользователем: $U \xrightarrow{C_{init}(U,DPL)} DPL$ угроза U вызвала сценарий DPL, при этом переменная $C_{init}(U, DPL)$ описывает вероятность инициализации сценария; $U \xrightarrow{C_{init}(U,FSS)} FSS$ угроза U вызвала сценарий FSS, при этом переменная $C_{init}(U, FSS)$ описывает вероятность инициализации сценария; $U \xrightarrow{C_{init}(U,FMS)} FMS$ угроза U вызвала сценарий FMS, при этом переменная $C_{init}(U, FMS)$ описывает вероятность инициализации сценария.

Отношения наследия между сценариями угроз: $DPL \xrightarrow{C_{Lt}(DPL,HSP)} HSP$ – реализации сценария DPL ведет к сценарию HSP, при этом переменная $C_{Lt}(DPL, HSP)$ описывает степень влияния сценария угрозы; $FSS \xrightarrow{C_{Lt}(FSS,VIP)} VIP$ – реализации сценария FSS ведет к сценарию VIP, при этом переменная $C_{Lt}(FSS, VIP)$ описывает степень влияния сценария угрозы; $FMS \xrightarrow{C_{Lt}(FMS,VIP)} VIP$ – реализации сценария FMS ведет к сценарию VIP, при этом переменная $C_{Lt}(FMS, VIP)$ описывает степень влияния сценария угрозы; $VIP \xrightarrow{C_{Lt}(VIP,HSP)} HSP$ – реализации сценария VIP ведет к сценарию HSP, при этом переменная $C_{Lt}(VIP, HSP)$ описывает степень влияния сценария угрозы.

Отношения наследия между сценариями угроз и нежелательными инцидентами: $HSP \xrightarrow{C_{Lt}(HSP,HEU)} HEU$ – реализация сценария HSP ведет к нежелательному инциденту HEU, при этом переменная $C_{Lt}(HSP, HEU)$ описывает степень влияния сценария угрозы; $VIP \xrightarrow{C_{Lt}(VIP,UDO)} UDO$ – реализация сценария VIP ведет к нежелательному инциденту UDO, при этом переменная $C_{Lt}(VIP, UDO)$ описывает степень влияния сценария угрозы; $VIP \xrightarrow{C_{Lt}(VIP,UGB)} UGB$ – реализация сценария VIP ведет к нежелательному инциденту UGB, при этом переменная $C_{Lt}(VIP, UDO)$ описывает степень влияния сценария угрозы; $VIP \xrightarrow{C_{Lt}(VIP,USS)} USS$ – реализации сценария VIP ведет к нежелательному инциденту USS, при этом

переменная $C_{Lt}(VIP, USS)$ описывает степень влияния сценария угрозы; $UDO \xrightarrow{C_{Lt}(UDO,HEU)} HEU$ – возникновение нежелательного инцидента UDO ведет к нежелательному инциденту HEU, при этом переменная $C_{Lt}(UDO, HEU)$ описывает степень влияния сценария угрозы.

Отношения влияния нежелательных инцидентов на активы системы: $HEU \xrightarrow{C_{imp}(HEU,Dc)} Dc$ возникновение нежелательного инцидента HEU влияет на оценку актива Dc, при этом переменная $C_{imp}(HEU, Dc)$ описывает степень влияния на актив; $HEU \xrightarrow{C_{imp}(HEU,SegA)} SegA$ – возникновение нежелательного инцидента HEU влияет на оценку актива $SegA$, при этом переменная $C_{imp}(HEU, SegA)$ описывает степень влияния на актив; $UDO \xrightarrow{C_{imp}(UDO,Udc)} Udc$ – возникновение нежелательного инцидента UDO влияет на оценку актива UDc, при этом переменная $C_{imp}(UDO, Udc)$ описывает степень влияния на актив; $UGB \xrightarrow{C_{imp}(UGB,NetA)} NetA$ – возникновение нежелательного инцидента UGB влияет на оценку актива $NetA$, при этом переменная $C_{imp}(UGB, NetA)$ описывает степень влияния на актив; $USS \xrightarrow{C_{imp}(USS,Uda)} Uda$ – возникновение нежелательного инцидента USS влияет на оценку актива Uda, при этом переменная $C_{imp}(USS, Uda)$ описывает степень влияния на актив.

Также, на работу системы могут повлиять некомпетентность или ошибки администраторов сети, влияние которых представлено на рис. Б.3.

Описание процессов диаграммы. В системе возможно разделение на администраторов, отвечающих за работоспособность телекоммуникационной составляющей системы, и отвечающих за работоспособность сервисов системы.

Администраторы сети могут допустить ошибки при настройке пограничного оборудования, системы мониторинга, локальных систем пользователей. Также возможна ошибку при управлении ключами системы. Администраторы сервисов могут некорректно организовать работу сервиса, что потенциально угрожает защите всей системы, а также допустить ошибки в клиентской части

приложений. Данные ошибки могут привести к уже указанным инцидентам осуществления доступа к серверам и сервисам, сети, данным корпорации и личным данным и т. д.

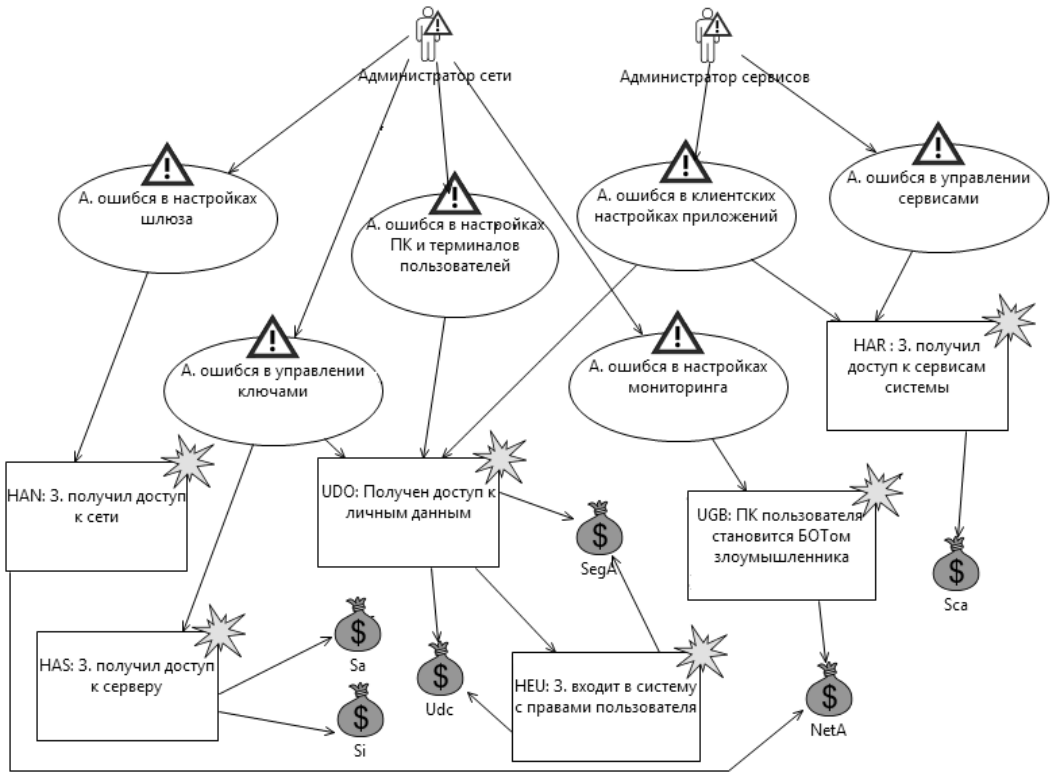


Рисунок Б.3 – Диаграмма угроз. Влияние администраторов

В данной диаграмме определены следующие элементы:

Угрозы: NA – администратор сети, SA - администратор сервисов.

Подмножество сценариев угроз: FGS – администратор ошибся в настройках шлюза; FCS – администратор ошибся в настройках ПК и терминалов пользователей; FKM – администратор ошибся в управлении ключами; FMM – администратор ошибся в настройках мониторинга; FAS – администратор ошибся в клиентских настройках приложений; FSM – администратор ошибся в управлении сервисами.

Подмножество нежелательных инцидентов пересекается с уже рассмотренными подмножествами.

Множество отношений следующее:

Отношения инициализации сценариев администраторами: $NA \xrightarrow{C_{init}(NA,FGS)} FGS$ – сценарий FGS вызван угрозой NA, при этом переменная $C_{init}(NA, FGS)$ описывает вероятность возникновения сценария; $NA \xrightarrow{C_{init}(NA,FCS)} FCS$ – сценарий FCS вызван угрозой NA, при этом переменная $C_{init}(NA, FCS)$ описывает вероятность возникновения сценария; $NA \xrightarrow{C_{init}(NA,FKM)} FKM$ – сценарий FKM вызван угрозой NA, при этом переменная $C_{init}(NA, FKM)$ описывает вероятность возникновения сценария; $NA \xrightarrow{C_{init}(NA,FMM)} FMM$ – сценарий FMM вызван угрозой NA, при этом переменная $C_{init}(NA, FMM)$ описывает вероятность возникновения сценария; $SA \xrightarrow{C_{init}(SA,FMM)} FMM$ – сценарий FMM вызван угрозой NA, при этом переменная $C_{init}(NA, FMM)$ описывает вероятность возникновения сценария; $SA \xrightarrow{C_{init}(SA,FSM)} FSM$ – сценарий FSM вызван угрозой NA, при этом переменная $C_{init}(NA, FSM)$ описывает вероятность возникновения сценария.

Отношения наследия между сценариями угроз и нежелательными инцидентами: $FGS \xrightarrow{C_{Lt}(FGS,HAN)} HAN$ – реализация сценария FGS ведет к нежелательному инциденту HAN, при этом переменная $C_{Lt}(FGS, HAN)$ описывает возможность данного следствия; $FKM \xrightarrow{C_{Lt}(FKM,HAS)} HAS$ – реализация сценария FKM ведет к нежелательному инциденту HAS, при этом переменная $C_{Lt}(FKM, HAS)$ описывает возможность данного следствия; $FKM \xrightarrow{C_{Lt}(FKM,UDO)} UDO$ – реализация сценария FKM ведет к нежелательному инциденту UDO, при этом переменная $C_{Lt}(FKM, UDO)$ описывает возможность данного следствия; $FCS \xrightarrow{C_{Lt}(FCS,UDO)} UDO$ – реализация сценария FCS ведет к нежелательному инциденту UDO, при этом переменная $C_{Lt}(FCS, UDO)$ описывает возможность данного следствия; $FAS \xrightarrow{C_{Lt}(FAS,UDO)} UDO$ – реалиизация сценария FAS ведет к нежелательному инциденту UDO, при этом переменная $C_{Lt}(FAS, UDO)$ описывает возможность данного следствия; $FAS \xrightarrow{C_{Lt}(FAS,HAR)} HAR$ – реализация сценария

FAS ведет к нежелательному инциденту HAR , при этом переменная $C_{Lt}(FAS, HAR)$ описывает возможность данного следствия; $FMM \xrightarrow{C_{Lt}(FMM,UGB)} UGB$ – реализация сценария FMM ведет к нежелательному инциденту UGB, при этом переменная $C_{Lt}(FMM, UGB)$ описывает возможность данного следствия; $FSM \xrightarrow{C_{Lt}(FSM,HAR)} HAR$ – реализация сценария FSM ведет к нежелательному инциденту HAR, при этом переменная $C_{Lt}(FSM, HAR)$ описывает возможность данного следствия.

Отношения влияния нежелательных инцидентов на активы системы:

$HAS \xrightarrow{C_{imp}(HAS,Si)} Si$ возникновение нежелательного инцидента HAS влияет на оценку актива Si, при этом переменная $C_{imp}(HAS, Si)$ описывает степень влияния на актив; $HAS \xrightarrow{C_{imp}(HAS,Sa)} Sa$ возникновение нежелательного инцидента HAS влияет на оценку актива Sa, при этом переменная $C_{imp}(HAS, Sa)$ описывает степень влияния на актив; $HAN \xrightarrow{C_{imp}(HAN,NetA)} NetA$ – возникновение нежелательного инцидента HAN влияет на оценку актива $NetA$, при этом переменная $C_{imp}(HAN, NetA)$ описывает степень влияния на актив; $UDO \xrightarrow{C_{imp}(UDO,Udc)} Udc$ – возникновение нежелательного инцидента UDO влияет на оценку актива UDc, при этом переменная $C_{imp}(UDO, Udc)$ описывает степень влияния на актив; $UDO \xrightarrow{C_{imp}(UDO,SegA)} SegA$ – возникновение нежелательного инцидента UDO влияет на оценку актива $SegA$, при этом переменная $C_{imp}(UDO, SegA)$ описывает степень влияния на актив; $UGB \xrightarrow{C_{imp}(UGB,NetA)} NetA$ – возникновение нежелательного инцидента UGB влияет на оценку актива $NetA$, при этом переменная $C_{imp}(UGB, NetA)$ описывает степень влияния на актив; $HEU \xrightarrow{C_{imp}(HEU,SegA)} SegA$ – возникновение нежелательного инцидента HEU влияет на оценку актива $SegA$, при этом переменная $C_{imp}(HEU, SegA)$ описывает степень влияния на актив; $HEU \xrightarrow{C_{imp}(HEU,Udc)} Udc$ – возникновение нежелательного инцидента HEU влияет на оценку актива Udc, при этом переменная

$C_{imp}(HEU, Udc)$ описывает степень влияния на актив; $HAR \xrightarrow{C_{imp}(HAR,Sca)} Sca$ – возникновение нежелательного инцидента HAR влияет на оценку актива Sca, при этом переменная $C_{imp}(HAR, Sca)$ описывает степень влияния на актив.

Приложение В

Структуры взаимодействия элементов риска

Структуры взаимодействия элементов были получены на основе построенных диаграмм Coras. Такие структуры могут строится самостоятельно при идентификации элементов риска.

На рисунке В.1 представлена структура для описания воздействия на актив $NetA$. Вершины $T = \{H, V, U, NA\}$ определяют источник угрозы как отправную точку. Сценарии угроз $TS = \{HPG, HSD, VIP, FSS, FMS, FMM, FGS\}$ активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы.

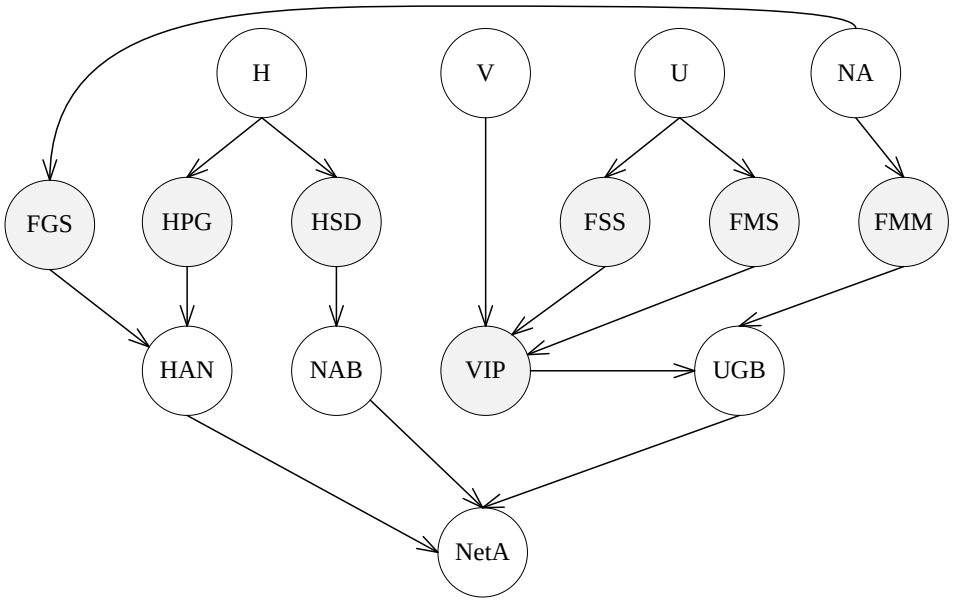


Рисунок В.1 – Структура взаимодействия элементов риска на актив NetA

Данные значения характеризуют степень возможности начала соответствующего сценария угрозы. Реализация сценариев угрозы приводит к одному из нежелательных инцидентов $UI = \{HAN, NAB, UGB\}$ с некоторым значением вероятности, зависящим от отношения наследия C_{Lt}.

На рисунке В.2 представлены структуры для описания воздействия на активы Si и Sa. Вершины $T = \{H, V, U, NA\}$ определяют источник угрозы как источники сценариев.

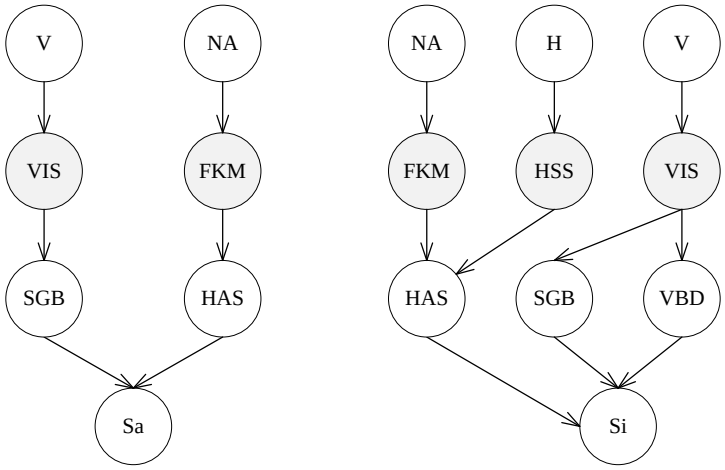


Рисунок В.2 – Структура взаимодействия элементов риска на активы Si и Sa

Сценарии угроз VIS, FKM, HSS активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы. Реализация сценариев угрозы приводит к одному из нежелательных инцидентов SGB, HAS, VBD с некоторым значением вероятности, зависящим от отношения наследия C_{Lt}.

На рисунке В.3 представлены иерархические системы для описания воздействия на активы *Di* и *Da*.

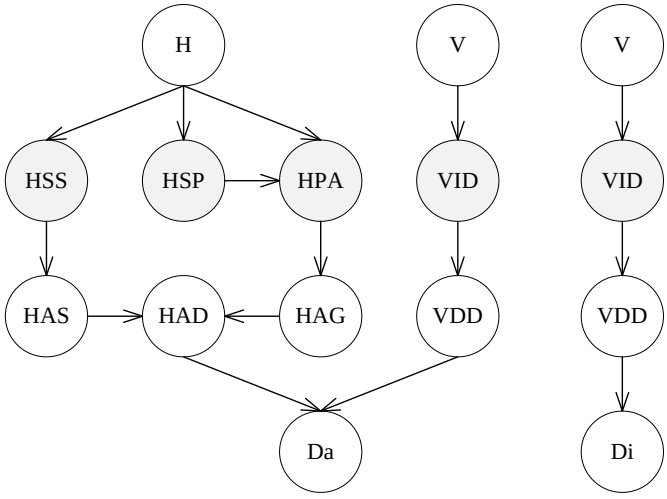


Рисунок В.3 – Структура взаимодействия элементов риска на активы Da и Di

Вершины H,V определяют источник угрозы как отправную точку. Сценарии угроз *VID,HSP,HPA,HSS* активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы. Реализация сценариев угрозы приводит к одному из нежелательных инцидентов *HAS, HAG, HAD,VDD* с некоторым значением вероятности, зависящим от отношения наследия C_{Lt}.

На рисунке В.4 представлена иерархическая система для описания воздействия на актив *Dc*.

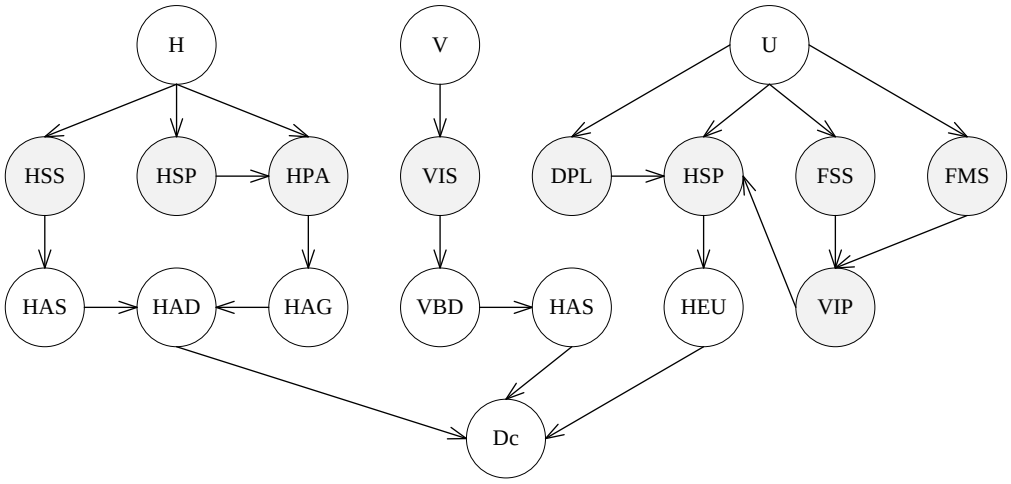


Рисунок В.4 – Структура взаимодействия элементов риска на актив Dc

Вершины *V,H,U* определяют источник угрозы как отправную точку. Сценарии угроз *VIS,DPL,FSS,FSM,HSS,HSP,HPA* активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы. Реализация сценариев угрозы приводит к одному из нежелательных инцидентов *HAS,HEU,HAG, HAD,VBD* с некоторым значением вероятности, зависящим от отношения наследия C_{Lt}.

На рисунке В.5 представлена иерархическая система для описания воздействия на актив *Sca*.

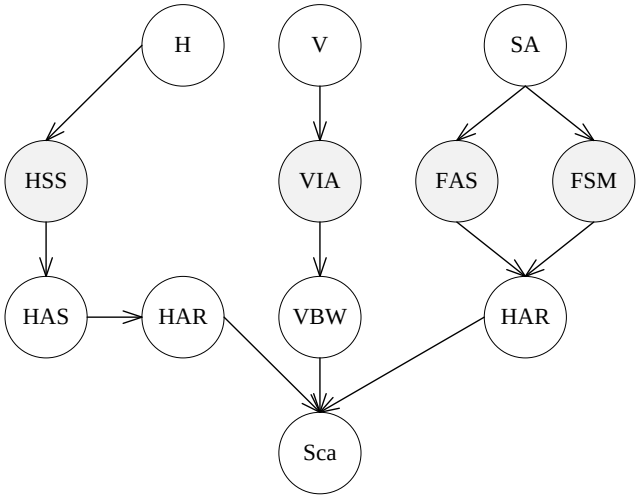


Рисунок В.5 – Структура взаимодействия элементов риска на актив Sca

Вершины *V,H,SA* определяют источник угрозы как отправную точку. Сценарии угроз *VIA,FAS,FSM,HSS* активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы. Реализация сценариев угрозы приводит к одному из нежелательных инцидентов *HAS,HAR,VBW* с некоторым значением вероятно-

сти, зависящим от отношения наследия C_{Lt}.

На рисунке В.6 представлена иерархическая система для описания воздействия на актив *SegA*.

Вершины *U,H,SA* определяют источник угрозы как отправную точку. Сценарии угроз *FAS,FSS,FMS,DPL,FKM,HSP,HPA* активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы. Реализация сценариев угрозы приводит к одному из нежелательных инцидентов *HAG,HEU,UDO* с некоторым значением вероятности, зависящим от отношения наследия C_{Lt}.

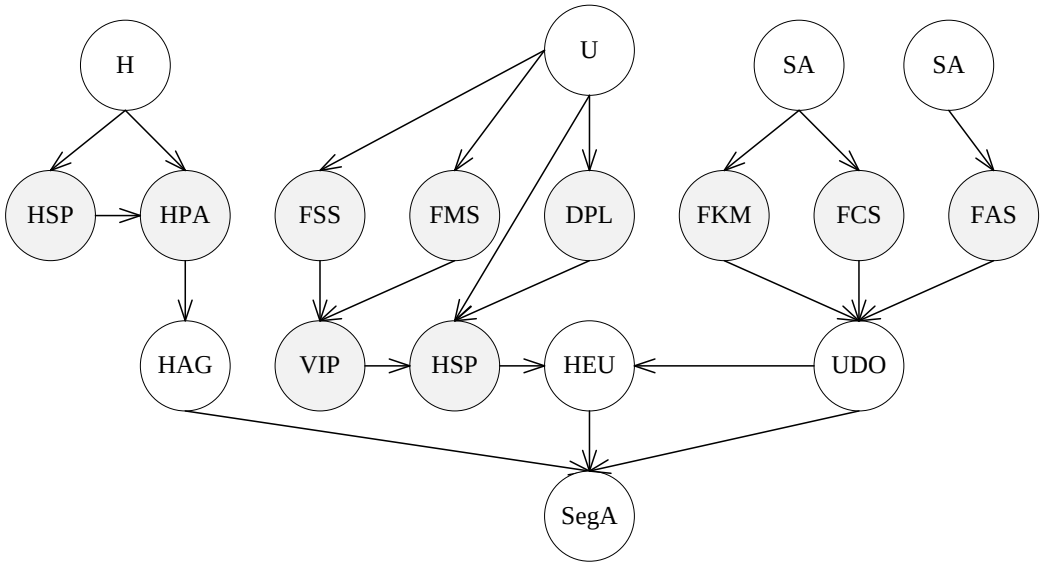


Рисунок В.6 – Структура взаимодействия элементов риска на актив SegA

На рисунке В.7 представлены иерархические системы для описания воздействия на активы *EqA,Uda*.

Вершины *U,H,V* определяют источник угрозы как отправную точку. Сценарии угроз *VIP,FSS,FMS,HSP,HPA* активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы.Реализация сценариев угрозы приводит к одному из нежелательных инцидентов *HAG,UGB,USS* с некоторым значением вероятности, зависящим от отношения наследия C_{Lt}.

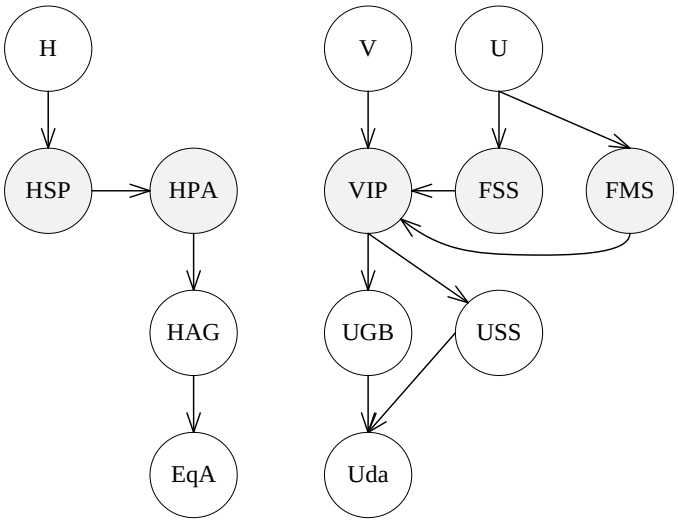


Рисунок В.7 – Структура взаимодействия элементов риска на активы Eqa и Uda

На рисунке В.8 представлены иерархические системы для описания воздействия на активы *EqI,Udc*. Вершины *U,H,V,SA,NA* определяют источник угрозы как отправную точку. Сценарии угроз *VIP,FSS,FMS,HSP,FCS, FKM,FAS* активизируются с некоторым значением вероятности, которое описывается отношением C_{init} от соответствующей угрозы.

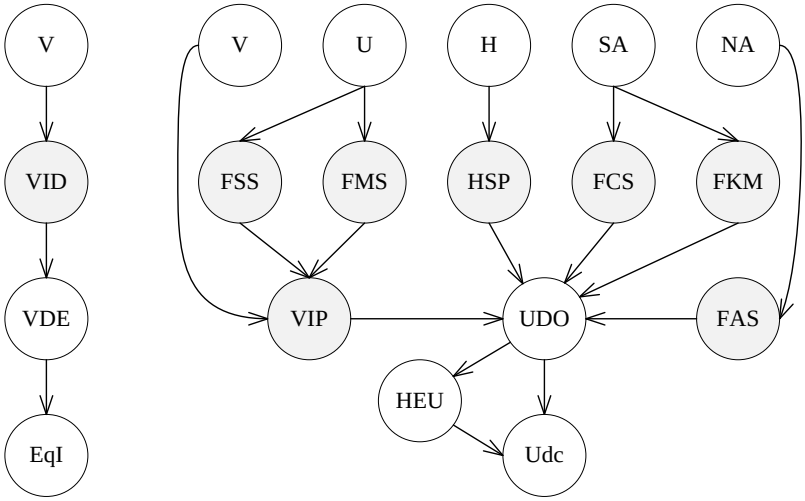


Рисунок В.8 – Структура взаимодействия элементов риска на активы EqI и Udc

Реализация сценариев угрозы приводит к одному из нежелательных инцидентов *VDE,UDO* с некоторым значением вероятности, зависящим от отношения наследия C_{Lt}.

Приложение Д

Модели сценариев угроз

Для моделирования сценария угрозы следует определить его структуру, т. е. этапы его реализации, параметры данных этапов и взаимное влияние этапов друг на друга.

В рамках работы были определены следующие сценарии:

а) сценарии, определяемые действиями злоумышленника:

– HSS – злоумышленник запустил на сервере свои сценарии;

– HSP – злоумышленник похитил логины и ключи пользователя;

– HPA – злоумышленник обошел правила доступа к сегментам;

– HPG – злоумышленник обошел правила доступа на шлюзе;

– HSD – злоумышленник провел DoS атаку на шлюз.

б) сценарии, определяемые деятельностью вируса:

– VIS – вирус инфицировал сервер;

– VID – вирус инфицировал устройства сегментов сети;

– VIA – вирус инфицировал приложения;

– VIP – вирус инфицировал пользовательские устройства.

в) сценарии, определяемые действиями пользователей:

– DPL – дискредитация логинов и паролей;

– HSP – злоумышленник похитил логины и пароли пользователя;

– FSS – некорректное использование поисковых систем;

– FMS – некорректное использование почтовых систем;

– VIP – вирус инфицировал пользовательские устройства.

г) сценарии, определяемые действиями администраторов системы:

– FGS – администратор сети ошибся в настройках шлюза;

– FKM – администратор сети ошибся в управлении ключами;

– FCS – администратор сети ошибся в настройках устройств польз.;

– FAS – администратор сервисов ошибся в клиентских настройках;

– FMS – администратор сети ошибся в настройках мониторинга;

– FSM – администратор сервисов ошибся в управлении сервисами.

Сценарии, связанные с действиями злоумышленника, представлены на рисунках Д.1-Д.5. Вершины графов представляют собой состояния, в которых находятся участники процессов или сама система, действия описывают деятельность этих участников.

Запуск злоумышленником сценариев на сервере, в общем виде, заключается в модификации входящих данных путем встраивания специальных команд или кода в запросы серверу.

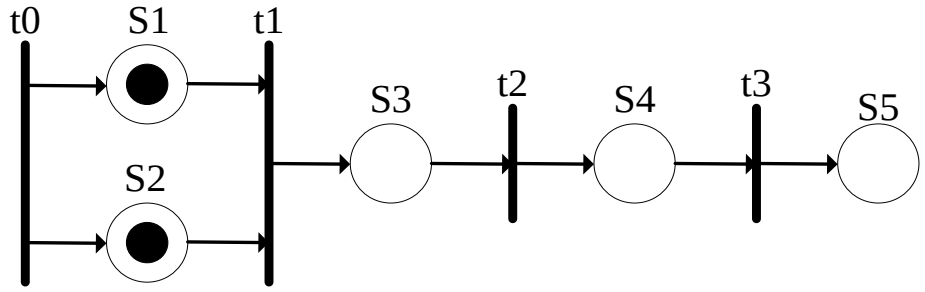


Рисунок Д.1 – модель сценария угрозы HSS

Здесь S1 – сервер готов принимать пакеты, S2 – З. готов к прослушиванию и перехвату пакетов, S3 – З. перехватил пакеты, S4 – сервер принял модифицированные пакеты, S5 – З. получил доступ к серверу, t0 – начальная задержка срабатывания сети, t1 – злоумышленник перехватывает входящие пакеты сервера, t2 – З. встраивает в пакеты свой код, t3 – встроенный код активирует заданных сценарий на сервере.

Последовательность t0-S1,S2-t1 представляет собой взаимное ожидание события, остальные элементы представляют собой последовательные переходы из состояния в состояние.

$$\tau_1(HSS) = \frac{\tau_{11}(HSS)^2 + \tau_{11}(HSS)\tau_{21}(HSS) + \tau_{21}(HSS)^2}{\tau_{11}(HSS) + \tau_{21}(HSS)}$$

$$\tau(HSS) = \tau_1(HSS) + \tau_{32}(HSS) + \tau_{43}(HSS)$$

$$\tau_{HSS} = FDEF(\tau(HSS))$$

$$P(HSS)(t) = 1 - e^{-t/\tau_{HSS}}$$

Параметры $\tau_{ij}(HSS)$ имеют следующий смысл: $\tau_{11}(HSS)$ – среднее время передачи пакетов серверу, $\tau_{21}(HSS)$ – среднее время перехвата пакетов злоумышленником, $\tau_{32}(HSS)$ – среднее время модификации перехваченных пакетов, $\tau_{43}(HSS)$ – среднее время срабатывания сценария на сервере. При этом, параметры τ_{ij} принимают следующие диапазоны значения:

– $\tau_{11}(HSS) \in [0.1, 0{,}4]c = [a_{11}(HSS), b_{11}(HSS)]$,

– $\tau_{21}(HSS) \in [0.2, 0{,}5]c = [a_{21}(HSS), b_{21}(HSS)]$,

– $\tau_{32}(HSS) \in [1, 3]c = [a_{32}(HSS), b_{32}(HSS)]$,

– $\tau_{43}(HSS) \in [1, 3]c = [a_{43}(HSS), b_{43}(HSS)]$.

Сценарий угрозы HSP (рис. Д.2) определяет действия, которые приводят к хищению идентификационных данных пользователей. В случае, когда злоумышленник целенаправленно занимается такой деятельностью, сценарий угрозы, в общем виде, сводится к ожиданию момента, когда пользователь произведет идентификацию на целевой системе, и перехвату данных, которые передает пользователь. После анализа полученных пакетов, злоумышленник имеет на руках идентификаторы и пароли пользователя.

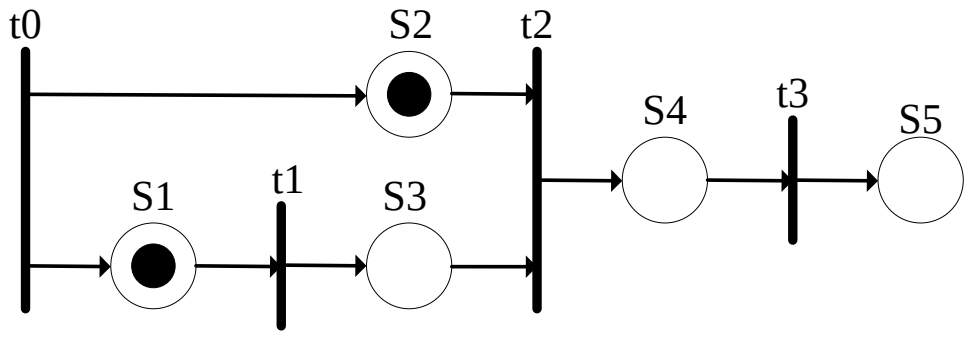


Рисунок Д.2 – Модель сценария угрозы HSP

В данной модели S1 – З. Находится в одной сети с пользователем, S2 –П. готов к идентификации, S3 – З. готов к перехвату пакетов, S4 – логин и пароль переданы серверу, пакеты прослушаны З., S5 – З. завладел логином и паролем пользователя, t1 – З. подготовил ПО для прослушивания, t2 – П. производит идентификацию, t3 – З. анализирует прослушанные пакеты и выявил пароль и логин.

Математическое описание данной модели имеет вид

$$\tau_1(HSP) = \tau_{11}(HSP) + \tau_{32}(HSP),$$

$$\tau_2(HSS) = \frac{\tau_1^2(HSS) + \tau_1(HSS)\tau_{22}(HSP) + \tau_{22}^2(HSP)}{\tau_1(HSP)+\tau_{22}(HSP)},$$

$$\tau(HSP) = \tau_2(HSP) + \tau_{43}(HSP),$$

$$\tau_{HSP} = FDEF\big(\tau(HSP)\big),$$

$$P(HSP) = 1 - e^{-t/\tau_{HSP}}$$

В данной модели параметры τ_{ij} имеют следующий смысл: τ_{11} – среднее время подготовки ПО, τ_{22} – среднее время идентификации пользователя, τ_{32} – среднее время перехвата пакетов, τ_{43} – среднее время анализа перехваченных пакетов. Нечеткие значения этих параметров следующие:

– $\tau_{11}(HSP) \in [10-15]c = [a_{11}(HSP), b_{11}(HSP)]$;

– $\tau_{22}(HSP) \in [5-10]c = [a_{22}(HSP), b_{22}(HSP)]$;

– $\tau_{32}(HSP) \in [0{,}2-0{,}6]c = [a_{32}(HSP), b_{32}(HSP)]$;

– $\tau_{43}(HSP) \in [5-30]c = [a_{43}(HSP), b_{43}(HSP)]$.

Действия, связанные с обходом правил доступа (к сегментам сети, к узловому оборудованию), зависят от реализации предыдущего сценария, так как успех данного сценария предусматривает либо хищение, либо подбор данных, которые соответствуют легальным пользователям и устройствам. Другим возможным сценарием развития может быть сканирование открытых соединений

из сегмента и соответствующих портов для протоколов. Данная схема изображена на рисунке Д.3.

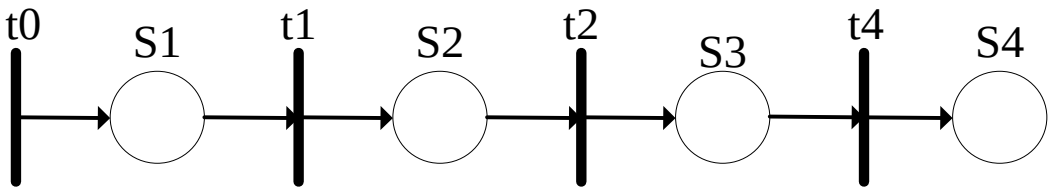


Рисунок Д.3 – Сценарий угрозы HPA

В данной модели S1 – 3. настроил ПОдля сканирования портов, S2 – обнаружены открытые соединения и порты этих соединений, S3 – определены активные хосты, S4 – 3. обошел ограничение доступа,t0 – задержка начального срабатывания сети, t1 – производится сканирование соединений и портов, t2 – определение активных конечных узлов сегмента, t3 – осуществление входа в систему. Описание данной модели имеет следующий вид

$$\tau(HPA) = \tau_{11}(HPA) + \tau_{22}(HPA) + \tau_{33}(HPA),$$
$$\tau_{HPA} = FDEF\big(\tau(HPA)\big),$$
$$P(HPA)(t) = 1 - e^{-t/\tau_{HPA}}$$

При этом параметры τ_{ij} имеют следующий смысл: τ_{11} –среднее время подготовки ПО, τ_{22} - среднее время обнаружения открытых соединений, портов, протоколов, τ_{33} - среднее время определения целевых хостов с открытыми соединениями. Данные параметры имеют следующие диапазоны значений:

– $\tau_{11}(HPA) \in [10 - 15]c = [a_{11}(HPA), b_{11}(HPA)]$,

– $\tau_{22}(HPA) \in [0{,}5 - 5]c = [a_{22}(HPA), b_{22}(HPA)]$,

– $\tau_{33}(HPA) \in [0{,}2 - 0{,}6]c = [a_{33}(HPA), b_{33}(HPA)]$.

Реализация сценария DoS атаки описана на рисунке Д.4

Здесь S1 – З. готов к проведению атаки, S2 – сервер готов принимать входящие пакеты, S3 – З. запустил и настроил ПО, S4 – запросы поставлены в очередь сервера, S5 – сервер не в состоянии обрабатывать запросы, t0 – начальная задержка срабатывания сети, t1 – запуск и настройка ПО для атаки, t2 – отправка запросов и постановка их в очередь, t3 – переполнение очереди на сервере.

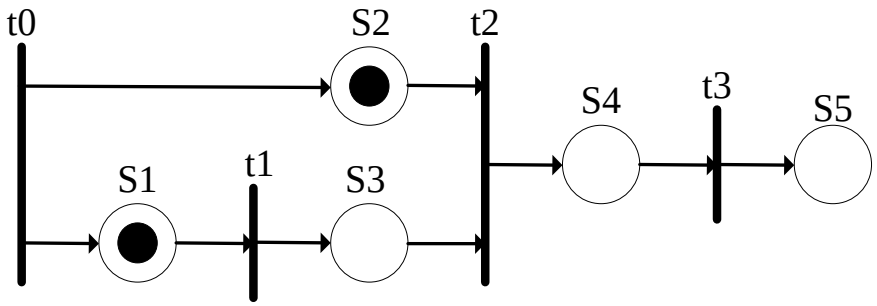


Рисунок Д.4 – Модель сценария DoS атаки (HSD)

Описание данной модели имеет следующий вид

$$\tau_1(HSD) = \tau_{11}(HSD) + \tau_{32}(HSD)$$

$$\tau_1(HSD) = \frac{\tau_1^2(HSD) + \tau_1(HSD)\tau_{22}(HSD) + \tau_{22}^2(HSD)}{\tau_1(HSD) + \tau_{22}(HSD)}$$

$$\tau(HSD) = \tau_2(HSD) + \tau_{43}(HSD)$$

$$\tau_{HSD} = FDEF\big(\tau(HSD)\big),$$

$$P(HSD)(t) = 1 - e^{-t/\tau_{HSD}}.$$

В данной модели параметры τ_{ij} имеют следующий смысл: τ_{11}–среднее время подготовки ПО, τ_{22} – среднее время приема пакетов сервером, τ_{32} - среднее время отправки запроса на соединение, τ_{43} – среднее время заполнения очереди сервера.

При этом параметры τ_{ij} принимают следующие диапазоны значений:

– $\tau_{11}(HSD) \in [10 - 15]c = [a_{11}(HSD), b_{11}(HSD)]$;

– $\tau_{22}(HSD) \in [0{,}015 - 0{,}02]c = [a_{22}(HSD), b_{22}(HSD)]$;

– $\tau_{32}(HSD) \in [0{,}001 - 0{,}015]c = [a_{32}(HSD), b_{32}(HSD)]$;

– $\tau_{43}(HSD) \in [0{,}1 - 0{,}2]c = [a_{43}(HSD), b_{43}(HSD)]$.

Вирусы представляют наибольший интерес, с точки зрения анализа рисков, так как все сценарии угроз, связанные с их деятельностью, так или иначе связаны со всеми участниками угроз.

Сценарии угроз осуществляемые посредством вирусов, представлены на рисунках Д.5 – Д.8

Сценарий, связанный с инфицированием вирусом устройств пользователя представлен на рисунке Д.5

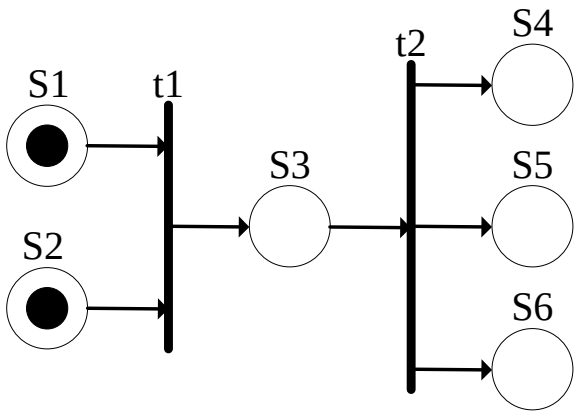


Рисунок Д.5 – Сценарий угрозы VIP

Здесь S1 – Сценарий угрозы FSS реализован, S2 – сценарий угрозы FMS реализован, S3 – вирус находится на устройстве пользователя, S4 – вирус получил доступ к подсистеме управления учетными записями, S5 – вирус получил доступ к подсистеме управления реестром и системными файлами, S6 – вирус получил доступ к подсистеме управления сетевых функций, t1 – вирус проникает в ОС на устройстве пользователя, t2 – вирус проникает в подсистемы ОС.

Математическое описание данной модели имеет следующий вид

$$\tau_1(VIP) = \frac{\tau_{11}(VIP) + \tau_{11}(VIP)\tau_{21}(VIP) + \tau_{21}(VIP)}{\tau_{11}(VIP) + \tau_{21}(VIP)}$$

$$\tau(VIP) = \tau_1(VIP) + \tau_{32}(VIP),$$
$$\tau_{VIP} = FDEF\big(\tau(VIP)\big),$$
$$P(VIP)(t) = 1 - e^{-t/\tau_{VIP}}.$$

В данной модели параметры имеют следующий смысл $\tau_{11}(VIP)$ – среднее время реализации сценария угрозы FSS, $\tau_{21}(VIP)$ – среднее время реализации сценария угрозы FMS, $\tau_{32}(VIP)$ - среднее время захвата вирусом подсистем операционной системы

Диапазоны значений для параметров модели следующие:

– $\tau_{11}(VIP) \in [\tau_{FSS}]$,

– $\tau_{22}(VIP) \in [\tau_{FMS}]$,

– $\tau_{33}(VIP) \in [0{,}25 - 1{,}5]c = [a_{33}(VIP), b_{33}(VIP)]$.

Сценарий, осуществляющий инфицирование сервера вирусом представлен на рисунке 3.6

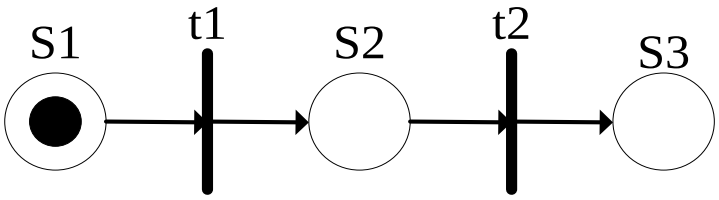


Рисунок Д.6 – Сценарий угрозы VIS

Здесь S1 – Сервер готов принимать пакеты; S2 – сервер принял входящие пакеты, среди них инфицированные вирусом; S3 – вирус находится на устройстве; t1 – сервер принимает входящие пакеты; t2 – вирус проникает в подсистемы сервера.

Математическое описание данной модели следующее

$$\tau(VIS) = \tau_{11}(VIS) + \tau_{22}(VIS)$$

$$\tau_{VIS} = FDEF\big(\tau(VIS)\big),$$

$$P(VIS)(t) = 1 - e^{-t/\tau_{VIS}}.$$

В данной модели параметры имеют следующий смысл $\tau_{11}(VIS)$ – среднее время приема пакетов сервером, $\tau_{22}(VIS)$ – среднее время распространения вируса по подсистемам сервера.

Данные параметры имеют следующие диапазоны значений:

– $\tau_{11}(VIS) \in [0{,}01 - 0{,}1]c = [a_{11}(VIS), b_{11}(VIS)]$,

– $\tau_{22}(VIS) \in [0{,}5 - 5]c = [a_{22}(VIS), b_{22}(VIS)]$.

Сценарий угрозы, осуществляющий инфицирование вирусом приложений системы, представлен на рисунке Д.7.

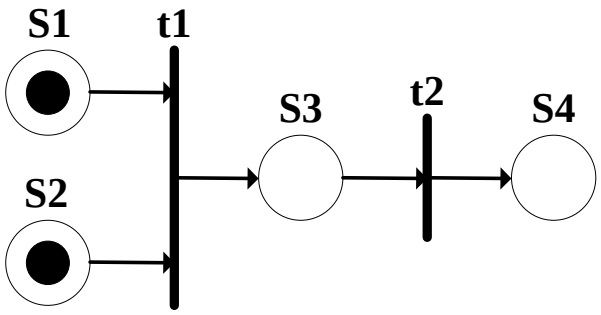


Рисунок Д.7 – Сценарий угрозы VIA

Здесь S1 – Приложение запущено и работает; S2 – пользователь готов к работе с приложением; S3 – пользователем переданы данные с интегрированным вирусом; S4 – вирус проникает на устройство; t1 – пользователь работает с приложением, производится обмен данными; t2 – вирус интегрирует в приложение или данные приложения.

Математическое описание данной модели следующее

$$\tau_1(VIA) = \frac{\tau_{11}(VIA) + \tau_{11}(VIA)\tau_{21}(VIA) + \tau_{21}(VIA)}{\tau_{11}(VIA) + \tau_{21}(VIA)},$$

$$\tau = \tau_1(VIA) + \tau_{32}(VIA),$$

$$\tau_{VIA} = FDEF\big(\tau(VIA)\big),$$

$$P(VIA)(t) = 1 - e^{-t/\tau_{VIA}}.$$

В данной модели параметры имеют следующий смысл $\tau_{11}(VIA)$ – среднее время запуска приложения, $\tau_{21}(VIA)$ – среднее время подготовки пользователя, $\tau_{32}(VIA)$ – среднее время работы приложения до инфицирования вирусом.

Данные параметры имеют следующие диапазоны значений:

– $\tau_{11}(VIA) \in [2-5]c = [a_{11}(VIA), b_{11}(VIA)]$,

– $\tau_{22}(VIA) \in [5-10]c = [a_{22}(VIA), b_{22}(VIA)]$,

– $\tau_{32}(VIA) \in [2-10]c = [a_{32}(VIA), b_{32}(VIA)]$.

Сценарий угрозы, осуществляющий инфицирование периферийных и специализированных устройств представлен на рисунке Д.8

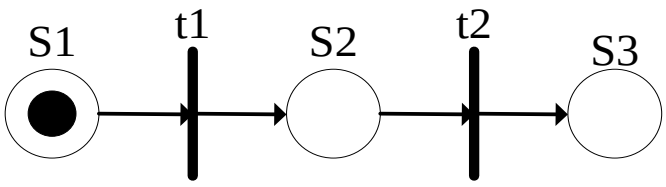


Рисунок Д.8 – Сценарий угрозы VID

Здесь S1 – Устройство готово к приему пакетов; S2 – вирус проник в системные сценарии устройства; S3 – устройство находится под контролем вируса; t1 – устройство принимает пакеты; t2 – вирус активизировал заданные сценарии.

Математическое описание данной модели следующее

$$\tau(VID) = \tau_{11}(VID) + \tau_{22}(VID),$$

$$\tau_{VID} = FDEF\big(\tau(VID)\big),$$

$$P(VID)(t) = 1 - e^{-t/\tau_{VID}}.$$

Параметры модели означают $\tau_{11}(VID)$ – среднее время приема пакетов устройством, $\tau_{22}(VID)$ – среднее время внедрения вируса.

Данные параметры имеют следующие диапазоны значений:

$$\tau_{11}(VID) \in [0{,}2 - 3]c = [a_{11}(VID), b_{11}(VID)],$$
$$\tau_{22}(VID) \in [0{,}5 - 4]c = [a_{22}(VID), b_{22}(VID)].$$

Пользователи представляют собой внутренние угрозы, которые, в общем случае, заключаются в неосторожном или неумелом обращении с компьютерной техникой или системой. Сценарии, связанные с угрозами пользователей представлены на рисунках Д.9 – Д.11.

Сценарий, связанный с неосторожным использованием почтовых систем представлен на рисунке Д.9.

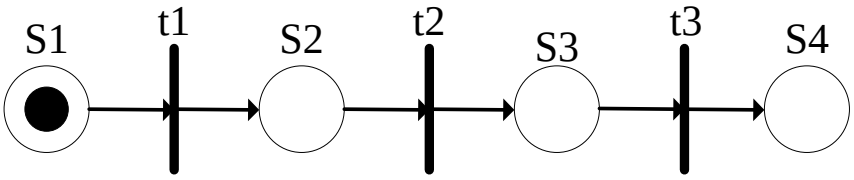


Рисунок Д.9 – Сценарий угрозы FMS

Здесь S1 – Пользователь готов к работе; S2 – поисковая система запущена; S3 – запрос обработан, ответ сформирован; S4 – вирус проникает на устройство; t1 – пользователь запускает поисковую систему; t2 – пользователь формирует запрос; t3 – пользователь активирует опасную ссылку.

Математическое описание данной модели следующее

$$\tau(FMS) = \tau_{11}(FMS) + \tau_{22}(FMS) + \tau_{33}(FMS),$$
$$\tau_{FMS} = FDEF\big(\tau(FMS)\big),$$
$$P(FMS)(t) = 1 - e^{-t/\tau_{FMS}}.$$

В данной модели параметры имеют следующий смысл $\tau_{11}(FMS)$ – среднее время подготовки к запуску поисковой системы, $\tau_{22}(FMS)$ – среднее время формулирования запроса, $\tau_{33}(FMS)$ – среднее время обработки запроса поисковой системы.

Данные параметры имеют следующие диапазоны значений:

– $\tau_{11}(FMS) \in [2-5]c = [a_{11}(FMS), b_{11}(FMS)]$,

– $\tau_{22}(FMS) \in [3-8]c = [a_{22}(FMS), b_{22}(FMS)]$,

– $\tau_{33}(FMS) \in [0{,}45-0{,}65]c = [a_{33}(FMS), b_{33}(FMS)]$.

Сценарий, описывающий неосторожную работу пользователя с почтовой системой, представлен на рисунке Д.10.

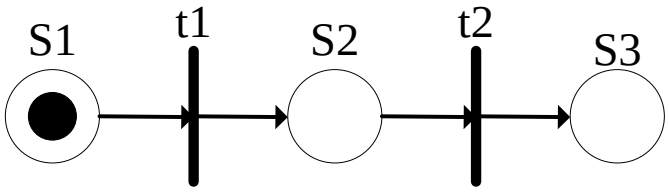


Рисунок Д.10 – Сценарий угрозы FSS

Здесь S1 – Пользователь готов к работе; S2 – Пользователь получил письмо; S3 – письмо со скрытым вирусом открыто; t1 – пользователь вошел в почтовую систему; t2 – пользователь открыл письмо.

Математическое описание данной модели следующее

$$\tau(FSS) = \tau_{11}(FSS) + \tau_{22}(FSS),$$
$$\tau_{FSS} = FDEF\big(\tau(FSS)\big),$$
$$P(FSS)(t) = 1 - e^{-t/\tau_{FSS}}.$$

В данной модели параметры означают следующее $\tau_{11}(FSS)$ – среднее время подготовки к запуску почтовой системы, $\tau_{22}(FSS)$ – среднее время просмотра и открытия письма.

Данные параметры имеют следующие диапазоны значений:

– $\tau_{11}(FSS) \in [2-5]c = [a_{11}(FSS), b_{11}(FSS)]$,

– $\tau_{22}(FSS) \in [5-10]c = [a_{22}(FSS), b_{22}(FSS)]$.

Сценарий, описывающий процессы утери или хищения паролей представлен на рисунке Д.11.

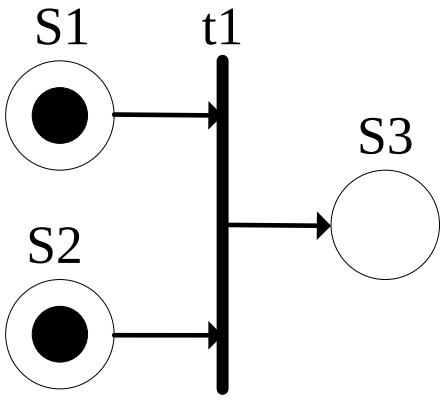


Рисунок Д.11 – Сценарий угрозы DPL

Здесь S1 – Пользователь готов к идентификации; S2 – злоумышленник или программа-шпион готовы к прослушиванию; S3 – данные переданы в открытом виде, или в непроверенную систему; t1 – пользователь проводит идентификацию и аутентификацию.

Математическое описание данной модели следующее

$$\tau(DPL) = \frac{\tau_{11}(DPL) + \tau_{11}(DPL)\tau_{21}(DPL) + \tau_{21}(DPL)}{\tau_{11}(DPL) + \tau_{21}(DPL)}$$

$$\tau_{DPL} = FDEF\big(\tau(DPL)\big),$$

$$P(DPL)(t) = 1 - e^{-t/\tau_{DPL}}.$$

Параметры модели означают следующее: $\tau_{11}(DPL)$ – среднее время процесса аутентификации, $\tau_{21}(DPL)$ – среднее время перехвата и анализа данных.

Данные параметры имеют следующие диапазоны значений:

– $\tau_{11}(DPL) \in [5-12]c = [a_{11}(DPL), b_{11}(DPL)]$;

– $\tau_{22}(DPL) \in [3-10]c = [a_{22}(DPL), b_{22}(DPL)]$.

Сценарии угроз VIP и HSP пересекаются с диаграммами для вируса и злоумышленника соответственно. Сами по себе сценарии идентичные, отличие заключается в условиях инициализации данных атак.