Министерство образования Республики Беларусь

Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ

Факультет Информационных технологий и управления
Кафедра Интеллектуальных информационных технологий

ОТЧЁТ

по ознакомительной практике

Выполнил: Я. Е. Лосик
Студент группы
321701
Проверил: Н. В. Малиновская

Минск 2024

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

ВВЕДЕНИЕ

Цель:

Закрепить практические навыки формализации информации в интеллектуальных системах с использованием семантических сетей.

Задачи:

- Построение формализованных фрагментов теории интеллектуальных компьтерных систем и технологий их разработки.
- Построение формальной семантической спецификации библиографических источников, соответствующих указанным выше фрагментам.
- Оформление конкретных методов и средств обеспечения безопасности традиционных информационных систем, особенностей обеспечения информационной безопасности интеллектуальных систем нового поколения.

1 ПОСТАНОВКА ЗАДАЧИ

Часть 2 Учебной дисциплины "Представление и обработка информации в интеллектуальных системах"

⇒ *библиографическая ссылка**:

- *монография OSTIS*
- *Материалы конференций OSTIS*
- *Исобоев Ш.И..ИнтелСМБСБСнОМО-2022ст*
  ⇒ *URL**:
  [https://cyberleninka.ru/article/n/vyyavlenie-riskov-ataki-chelovek-poseredine-v-sisteme-retranslyatsii-vpn-gate]
- *Скрыпников А.В..РешенЗИБсИ-2021ст*
  ⇒ *URL**:
  [https://cyberleninka.ru/article/n/realizatsiya-funktsiy-informatsionnoy-bezopasnosti-na-baze-servisov-infrastruktury-open-grid-services-architecture-ogsa.pdf]
- *Частикова В.А..МетодПСАИ-2022ст*
  ⇒ *URL**:
  [https://ntk.kubstu.ru/data/mc/0087/4347.pdf]
- *Абдурахман Д.Д.ИскусИиМОвК-2022ст*
  ⇒ *URL**:
  [https://elib.psu.by/bitstream/123456789/38126/1/341-345.pdf]
- *Остроух А.В.ИнтелСМ-2020кн*
  ⇒ *URL**:
  [http://nkras.ru/arhiv/2020/ostroukh1.pdf]
- *Баранович А.Е.СеманАИБКЗ-2011ст*
  ⇒ *URL**:
  [https://cyberleninka.ru/article/n/17313967.pdf]
- *Хоанг В.К..РешенОЗвРППБРсСБД-2013ст*
  ⇒ *URL**:
  [https://cyberleninka.ru/article/n/resheniya-osnovnyh-zadach-v-razrabotke-programmy-podderzhki-bezopasnosti-raboty-s-semanticheskimi-bazami-dannyh]
- *Голенков В.В..СеманМПиОБ-2017ст*
  ⇒ *URL**:
  [https://libeldoc.bsuir.by/handle/123456789/29503]
- *Дементьев А.В.МетриСД-2022ст*
  ⇒ *URL**:
  [https://moluch.ru/archive/419/93259/]
- *Golenkov V.V.Metho aTfECoC-2019art*
  ⇒ *URL**:
  [https://libeldoc.bsuir.by/handle/123456789/34574]
- *Дружинин В.Н..КогниПУдВ-2002кн*
  ⇒ *URL**:
  [https://adpuquba.edu.az/wp-content/uploads/2020/12/Koqnativnaya-Psixologiya-DRUJININA-rusca.pdf]
- *Созинова Е.Н.ПримеЭСдАиОИБ-2011ст*
  ⇒ *URL**:

[https://moluch.ru/archive/33/3766/]

Вопрос 1 по Части 2 Учебной дисциплины "Представление и обработка информации в интеллектуальных системах"

:= [Решение вопроса интеграции компьютерных систем]

⇒ *библиографическая ссылка**:

- *Golenkov V.V..Metho aTfECoC-2019art*
  - := [Methods and tools for ensuring compatibility of computer systems]

Вопрос 2 по Части 2 Учебной дисциплины "Представление и обработка информации в интеллектуальных системах"

:= [Экосистема ОСТИС]

⇒ *библиографическая ссылка**:

- *Обеспечение информационной безопасности в рамках Экосистемы OSTIS*
  - ∈ *раздел монографии*

Вопрос 3 по Части 2 Учебной дисциплины "Представление и обработка информации в интеллектуальных системах"

:= [Понятие интеллектуальных систем и технологий]

⇒ *библиографическая ссылка**:

- *Остроух А.В.ИнтелСМ-2020кн*
  - := [Интеллектуальные системы]

Вопрос 4 по Части 2 Учебной дисциплины "Представление и обработка информации в интеллектуальных системах"

:= [Обеспечение защиты интеллектуальной системы и технологий. Методы защиты интеллектуальных систем и технологий]

⇒ *библиографическая ссылка**:

- *Хоанг В.К..РешенОЗвРППБРсСБД-2013ст*
  - := [Решения основных задач в разработке программы поддержки безопасности работы с семантическими базами данных]

Вопрос 5 по Части 2 Учебной дисциплины "Представление и обработка информации в интеллектуальных системах"

:= [Применение экспертных систем]

⇒ *библиографическая ссылка**:

- *Созинова Е.Н.ПримеЭСдАиОИБ-2011ст*
  - ∈ *Применение экспертных систем для анализа и оценки информационной безопасности*

Вопрос 6 по Части 2 Учебной дисциплины "Представление и обработка информации в интеллектуальных системах"

:= [Когнитивная психология]

⇒ *библиографическая ссылка**:

- *Дружинин В.Н..КогниПУдВ-2002кн*
  - := [Когнитивная психология]

2 ФОРМАЛИЗОВАННЫЕ ФРАГМЕНТЫ ТЕОРИИ ИНТЕЛЛЕКТУАЛЬНЫХ КОМПЬТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ ИХ РАЗРАБОТКИ

Обеспечение информационной безопасности в рамках Экосистемы OSTIS

⇒ *аннотация**:

[В главе рассмотрены методы и средства обеспечения безопасности традиционных информационных систем, особенности обеспечения информационной безопасности интеллектуальных систем нового поколения (см. Главу 1.2. Интеллектуальные компьютерные системы нового поколения) и принципы, лежащие в основе обеспечения информационной безопасности ostis-систем.]

⇒ *библиографическая ссылка**:

- *Исобоев Ш.И..ИнтелСМБСБСнОМО-2022ст*
- *Скрыпников А.В..РешенЗИБсИ-2021ст*
- *Частикова В.А..МетодПСАИ-2022ст*
- *Абдурахман Д.Д.ИскусИиМОвК-2022ст*
- *Остроух А.В.ИнтелСМ-2020кн*
- *Баранович А.Е.СеманАИБКЗ-2011ст*
- *Хоанг В.К..РешенОЗвРППБРсСБД-2013ст*
- *Голенков В.В..СеманМПиОБ-2017ст*
- *Дементьев А.В.МетриСД-2022ст*
- *Golenkov V.V.Metho aTfECoC-2019art*
- *Дружинин В.Н..КогниПУдВ-2002кн*
- *Созинова Е.Н.ПримеЭСдАиОИБ-2011ст*

⇒ *Введение в главу 7.9**:

[Большое разнообразие моделей обеспечения информационной безопасности, всё возрастающий объем данных, которые необходимо анализировать для обнаружения атак на информационные системы, изменчивость методов атак и динамическое изменение защищаемых информационных систем, необходимость оперативного реагирования на атаки, нечеткость критериев обнаружения атак и выбора методов и средств реагирования на них, нехватка высококвалифицированных специалистов по защите влечет за собой потребность в использовании методов Искусственного интеллекта для решения задач безопасности]

2.1 Специфика обеспечения информационной безопасности интеллектуальных систем нового поколения

Информационная безопасность интеллектуальных систем

⊂ *Информационная безопасность*

⇒ *декомпозиция:**:

{
- *применение искусственного интеллекта в информационной безопасности*
- *организация информационной безопасности в интеллектуальных системах*

}

Искусственный интеллект

⇒ *применения:**:

{• *визуальное восприятие, распознавание речи, принятие решений и перевод с одного языка на другой.*
• *обнаружение вторжений*
:= [Искусственный интеллект может обнаруживать сетевые атаки, заражения вредоносным программным обеспечением и другие киберугрозы.]
• *кибераналитика*
:= [Искусственный интеллект также используется для анализа больших данных с целью выявления закономерностей и аномалий в системе кибербезопасности организации с целью обнаружения не только известных, но и ещё неизвестных угроз.]
• *безопасная разработка программного обеспечения*
:= [Искусственный интеллект может помочь создать более безопасное программное обеспечение, предоставляя разработчикам обратную связь в режиме реального времени.]
}
⇒ *классы:**:
{• *UEBA*
:= [User and Entity Behavior Analytics]
:= [Система анализа поведения субъектов (пользователей, программ, агентов) на предмет обнаружения нестандартного поведения и использования их для обнаружения потенциальных угроз с использованием шаблонов угроз (паттернов).]
• *TIP*
:= [Threat Intelligence Platform]
:= [Платформы раннего обнаружения угроз на основе сбора и анализа информации индикаторов компрометации и реагирования на них. Применение методов машинного обучения повышает эффективность обнаружения неизвестных угроз на ранних этапах.]
• *EDR*
:= [Endpoint Detection and Response]
:= [Системы обнаружения атак оперативного реагирования на конечных точках компьютерной сети. Могут обнаруживать вредоносные программы, автоматически классифицировать угрозы и самостоятельно реагировать на них.]
• *SIEM*
:= [Security Information and EventManagement]
:= [Системы сбора и анализа информации о событиях безопасности от сетевых устройств и приложений в реальном времени и оповещения]
• *NDR*
:= [Network Detection and Response]
:= [Системы обнаружения атак на сетевом уровне и оперативного реагирования на них. Искусственный интеллект использует на- копленную статистику и базу знаний об угрозах.]
• *SOAR*
:= [Security Orchestration and Automated Response]
:= [Системы, позволяющие выявлять угрозы информационной безопасности и автоматизировать реагирование на инциденты. В решениях данного типа, в отличие от SIEM-систем, Искусственный интеллект помогает не только проводить анализ, но и автоматически реагиро-

вать надлежащим образом на выявленные угрозы.]

- *Application Security*
  - := [Средства защиты приложений]
  - := [Системы, позволяющие определять угрозы безопасности прикладных приложений, управлять процессом мониторинга и устранения таких угроз.]
- *Antifraud*
  - := [Антифрод]
  - := [Платформы в режиме реального времени обнаруживают угрозы в бизнес-процессах и мошеннические операции. Искусственный интеллект используется для определения отклонений от идентифицированных бизнес-процессов с целью выявления вторжений или уязвимости процессов и повышает адаптивность к изменению логики и метрик бизнес-процессов.]

}

⇒ *недостатки**:

{
- *наборы данных, которые должны быть сформированы из значительного количества входных выборок, что требует много времени и ресурсов*
- *требуется огромное количество ресурсов, включая память, данные и вычислительную мощность*
- *частые ложные срабатывания, которые нарушают работу и в целом снижают эффективность таких систем*
- *организованные атаки на основе Искусственного интеллекта (семантические вирусы)*

}

Организация информационной безопасности в интеллектуальных системах нового поколения

Информационная безопасность

⇒ *поколения**:

{
- *Традиционные*
- *Нового поколения*

}

Информационная безопасность в традиционных интеллектуальных системах

⇒ *цели**:

{
- *обеспечение конфиденциальности информации в соответствии с проведенной классификацией*
- *обеспечение целостности информации на всех этапах, связанных с нею процессов (создание, обработка, хранение, передача и уничтожение) при предоставлении публичных услуг*
- *обеспечение своевременной доступности информации при предоставлении публичных услуг*
- *обеспечение наблюдаемости, направленной на фиксирование любой деятельности пользователей и процессов*
- *обеспечение аутентичности и невозможности отказа от транзакций и действий, производимых участниками предоставления публичных услуг*
- *учет всех процессов и событий, связанных с вводом, обработкой, хранением, предоставлением и уничтожением данных*

}

Информационная безопасность в интеллектуальных системах нового поколения

⇒ *цели**:

{• *обеспечение сохранности семантической совместимости информации*

• *защита достоверности и целостности информации*

• *обеспечение доступности информации на разных уровнях интеллектуальной системы*

• *минимизация ущерба от событий, несущих угрозу информационной безопасности*

}

⇒ *принципы**:

{• *Принцип равнопрочности*

:= [Означает обеспечение защиты оборудования, программного обеспечения и системы управления от всех видов угроз.]

• *Принцип непрерывности*

:= [Предусматривает непрерывное обеспечение безопасности информационных ресурсов системы для непрерывного предоставления публичных услуг.]

• *Принцип разумной достаточности*

:= [Означает применение таких мер и средств защиты, которые являются разумными, рациональными и затраты на которые, не превышают стоимости последствий нарушения информационной безопасности.]

• *Принцип комплексности*

:= [Для обеспечения безопасности во всем многообразии структурных элементов, угроз и каналов несанкционированного доступа должны применяться все виды и формы защиты в полном объеме.]

• *Принцип комплексной проверки*

:= [Заключается в проведении специальных исследований и проверок, специального инженерного анализа оборудования, верификационных исследований программных средств. Должен осуществляться непрерывный мониторинг аварийных сообщений и параметров ошибок, постоянно должно выполняться тестирование аппаратного и программного оборудования, а также контроль целостности программных средств, как при загрузке программных средств, так и в процессе функционирования.]

• *Принцип надежности*

:= [Методы, средства и формы защиты должны надежно перекрывать все пути проникновения и возможные каналы утечки информации, для этого допускается дублирование средств и мер безопасности.]

• *Принцип надежности*

:= [Меры безопасности должны перекрывать пути угроз независимо от места их возможного воздействия.]

• *Принцип плановости*

:= [Планирование должно осуществляться путем разработки детальных планов действий по обеспечению информационной защищенности всех компонент системы предоставления публичных услуг.]

• *Принцип централизованного управления*

:= [В рамках определенной структуры должна обеспечиваться организованно-функциональная самостоятельность процесса обеспечения безопасности при предоставлении публичных услуг.]

- *Принцип целенаправленности*
  ≔ [Необходимо защищать то, что должно защищаться в интересах конкретной цели.]
- *Принцип активности*
  ≔ [Защитные меры обеспечения безопасности в работе процесса предоставления услуг должны претворяться в жизнь с достаточной степенью настойчивости.]
- *Принцип квалификации обслуживающего персонала*
  ≔ [Обслуживание оборудования должно осуществляться сотрудниками, подготовленными не только в вопросах эксплуатации техники, но и в технических вопросах обеспечения безопасности информации.]
- *Принцип ответственности*
  ≔ [Ответственность за обеспечение информационной безопасности должна быть ясно установлена, передана соответствующему персоналу и утверждена всеми участниками в рамках процесса обеспечения информационной безопасности.]

}

2.2 Принципы, лежащие в основе обеспечения информационной безопасности ostis-систем

Экосистема OSTIS

⇒ *определение**:

[Сообщество, где происходит взаимодействие ostis-систем и пользователей, где должны быть установлены правила, которые должны контролироваться.]

⇒ *пояснение**:

[Нельзя допускать противоправные и дестабилизирую- щие действия со стороны всех участников сообщества. Пользователь не может на прямую осуществлять взаимодействия с другими ostis-системами, а только через персонального агента. Этот агент хранит все персональные данные пользователя и доступ к ним должен быть ограничен. В Экосистеме OSTIS все агенты должны быть идентифицированы. Следует отметить, что персональный агент пользователя в Экосистеме решает проблему идентификации самого пользователя. В рассмотренной Экосистеме OSTIS требуется организация обеспечения информационной безопасности на каждом из уровней взаимодействия: обмен данными, права доступа к данным, аутентификация клиентов Экосистемы, шифрование данных, получение данных из открытых источников, обеспечение достоверности и целостности хранимых и передаваемых данных, контроль за нарушением связей в базе знаний, отслеживание уязвимостей в системе.]

угроза в ostis-системе

⊃ *угроза. нарушение конфиденциальности информации*

⇒ *пояснение**:

[Несанкционированное получение доступа к чтению информации.]

⊃ *угроза. нарушение целостности информации*

⇒ *пояснение**:

[Несанкционированное или ошибочное изменение, искажение или уничтожение информации, а также несанкционированные воздействия на технические и программные средства об- работки информации.]

⊃ *угроза. нарушение доступности*

⇒ *пояснение**:

[Блокирование доступа к системе, отдельным ее компонентам, функциям или информации, а также невозможность своевременного получения информации (неприемлемые задержки в получении информации).]

⊃ *угроза. нарушение семантической совместимости*

⇒ *пояснение**:

[Нарушение общности понятий и в общности базовых знаний.]

⊃ *угроза. разрушение семантики баз знаний (семантические вирусы)*

⇒ *пояснение**:

[Подмена или удаление узлов и связей между ними в базе знаний.]

⊃ *угроза. избыточный объем входящей информации*

⊃ *угроза. нарушение неотказуемости*

⇒ *пояснение**:

[Выдача несанкционированных действий за легальные, а также сокрытие или подмена информации о действиях субъектов.]

⊃ *угроза. нарушение подотчетности*

⇒ *пояснение**:

[Несанкционированное или ошибочное изменение, искажение или уничтожение информации о выполнении действий субъектом.]

⊃ *угроза. нарушение подлинности (аутентичности)*

⇒ *пояснение**:

[Выполнение действий в системе от имени другого лица или выдача недостоверных ресурсов (в том числе и данных) за подлинные.]

⊃ *угроза. нарушение достоверности*

⇒ *пояснение**:

[Преднамеренное или непреднамеренное предоставление и использование ошибочной (неправильной) или неактуальной (на конкретный момент времени) информации, а также выполнение процедур в нарушении регламента (протокола).]

Информационная безопасность ostis-систем

⇒ *направления обеспечения безопасности**:

{• *ограничение информационного трафика, анализируемого интеллектуальной системой*

• *политика разграничении доступа к базе знаний*

• *связность*

• *введение семантической метрики*

• *семантическая совместимость*

• *активность*

}

⇒ *принципы**:

{• *Ограничение информационного трафика, анализируемого интеллектуальной системой*

:= [Экспоненциальный рост объема информации, циркулирующей в информационных потоках и ресурсах в условиях вполне определенных количественных ограничений на возможности средств ее восприятия, хранения, передачи и преобразования формирует новый класс угроз информационной безопасности, характеризуемых избыточностью совокупного входящего информационного трафика

интеллектуальных систем.]

- *Политика разграничении доступа к базе знаний*
  := [Мандатная политика безопасности (MAC — mandatory access control) основывается на мандатном (принудительном) разграничении доступа, определяющемся четырьмя условиями: все субъекты и объекты системы идентифицируются; задается решетка уровней безопасности информации; каждому объекту системы присваивается уровень безопасности, определяющий важность содержащейся в нем информации; каждому субъекту системы присваивается уровень доступа, определяющий уровень доверия к нему в интеллектуальной системе.]
- *Связность*
  := [Вся информация, хранимая в семантической памяти интеллектуальной системы, систематизирована в виде единой базы знаний.]
- *Введение семантической метрики*
  := [На множестве информационных единиц в некоторых случаях полезно задавать отношение, характеризующее семантическую близость информационных единиц, то есть силу ассоциативной связи между информационными единицами [7].]
- *Семантическая совместимость*
  := [Внутренняя семантическая совместимость между компонентами интеллектуальной компьютерной системы (максимально возможное введение общих, совпадающих понятий для различных фрагментов хранимой базы знаний), являющаяся формой конвергенции и глубокой интеграции внутри интеллектуальной компьютерной системы для различного вида знаний и различных моделей решения задач, что обеспечивает эффективную реализацию мультимодальности интеллектуальной компьютерной системы.]
- *Активность*
  := [Для интеллектуальных систем нового поколения можно выде- лить ряд аспектов, в рамках которых требуется работка новых алгоритмов и методов обеспечения информационной безопасно- сти в дополнении к существующим механизмам:
    - многоуровневый доступ к отдельным частям базы знаний, так как информация бывает общедоступной, персональной, конфиденциальной
    - мониторинг изменений значений слов с течением времени, а также значений перевода с иностранного языкакоторые мо- гут влиять на принимаемые решения
    - защиты от несанкционированного использования путем применения криптосемантических шифров
    - постоянный мониторинг уязвимостей в системе
    - протоколирование действий (взаимодействий) системы

  ]

}

Заключение

Для эффективной информационной защиты системы на современном этапе необходим симбиоз традиционных технологий, и технологий, реализуемых в рамках OSTIS. Также следует отметить, что обеспечение информационной безопасности на базе Технологии OSTIS осуществляется значительно проще, потому что многие аспекты уже реализованы на этапе проектирования самой технологии. Важно отметить, что интеллектуальная информационная система нового поколения — это самостоятельный субъект, который может сам осознанно, целенаправленно и постоянно заботиться о себе, в том числе о своей собственной безопасности.

3 ФОРМАЛЬНАЯ СЕМАНТИЧЕСКАЯ СПЕЦИФИКАЦИЯ БИБЛИОГРАФИЧЕСКИХ ИСТОЧНИКОВ

Golenkov V.V..Metho aTfECoC-2019art

⇒ *ключевой знак**:

- *семантическая компьютерная система;*
- *семантическая технология;*
- *гибридные системы;*
- *совместимость компьютерных систем;*
- *OSTIS-технология;*
- *SC-код;*
- *онтология*

⇒ *тип источника**:

[статья]

⇒ *аннотация**:

[Работа содержит описание методов и средств обеспечения совместимости компьютерных систем.]

⇒ *цитата**:

[

- **расширение набора и разнообразия проблем**, решенных компьютерной системой.
- снизить сложность этих проблем к проблемам сложно формализованным (сложно решаемым(осиливаемым, подумаю, что лучше, а лучше спрошу)), ителлектуальным проблемам решенным в условиях неполноценности, неточности, расплывчатости и т.д.
- улучшить качество решения проблем более эффективным использованием известных моделей для решения проблем(например, разработкой лучших алгоритмов) или использованием фундаментально новым моделей для решения проблем.
- расширение разнообразия используемой информации (знаний)
- расширение разнообразия используемых для решения проблем моделей

]

⇒ *принцип**:

[эволюция компьютерных систем]

⇒ *цитата**:

[Второе общее направление эволюции компьютерных систем – это улучшение их обучаемости и, как результат, темпа их эволюции.]

⇒ *принцип**:

[эволюция компьютерных систем]

⇒ *цитата**:

[Сущность нашего подхода к решению проблем эволюции компьютерных систем заключается, во-первых, в том, чтобы объединить все вышеперечисленные направления эволюции компьютерных систем (как общего направления, так и частного) и, во-вторых, осмыслить проблему обеспечения совместимости типов знаний, различных моделей решения проблем, различные компьютерные системы как ключевых проблем эволюции компьютерных систем, чьи решения значительно упростят решение многих других проблем.]

⇒ *принцип**:

[решение проблем компьютерных систем]

⇒ *цитата**:

[Однако логическую эквивалентность конструкций, хранящихся в памяти, не следует отбрасывать, поскольку логически эквивалентные знаковые конструкции являются репрезентациями одного и того же знания, но с помощью разных наборов понятий. Напротив, семантические конструкции эквивалентных знаков представляют собой представление одних и те же знаний с помощью одних и тех же понятий. Очевидно, что разнообразие возможных вариантов представления одних и тех же знаний в памяти компьютерных систем существенно усложняет задач решение.]

⇐ *сравнение**:

{• *логическая конструкция;*
• *семантическая конскрукция*
}

⇒ *цитата**:

[Как стандарт универсального смыслового представления информации в памяти компьютерных систем мы предложили SC-код (семантический компьютерный код).]

⇒ *пояснение**:

[SC-код]

⇒ *цитата**:

[Семейство всех введенных классов изучаемых объектов (включая максимальный класс) интерпретируется как Алфавит SC-кода. Но, в отличие от других языков, классы синтаксически выделенные элементарные фрагменты текстов кода СК могут перекрываться. Например, sc-элемент может принадлежат как классу sc-элемент, так и sc-вершина класс, а также может принадлежать классу sc-элемент и sc-коннектор, классу sc-дуги и базовому sc-дуге классу]

⇐ *сравнение**:

{• *Алфавит SC-кода;*
• *остальные языки*
}

⇒ *цитата**:

[Семейство всех введенных классов изучаемых объектов (включая максимальный класс) интерпретируется как Алфавит SC-кода. Но, в отличие от других языков, классы синтаксически выделенные элементарные фрагменты текстов кода СК могут перекрываться. Например, sc-элемент может принадлежат как классу sc-элемент, так и sc-вершина класс, а также может принадлежать классу sc-элемент и sc-коннектор, классу sc-дуги и базовому sc-дуге классу

Эта особенность Алфавита SC-кода позволяет строить синтаксически правильные SC-тексты (тексты SC-кода) в условиях неполноты нашего исходного знания о некоторых sc-элементах.]

⇒ *принцип**:

[Алфавит SC-кода]

⇒ *цитата**:

[Рассмотрим денотационную семантику sc-элементов принадлежность к разным синтаксически выделенным классам sc-элементов, т.е. имеющих разные синтаксические метки. Если sc-элемент помечен как sc-элемент, то он может обозначают любую описываемую сущность. Если sc-элемент имеет метку sc-коннектора, которая инцидентный sc-элементу ei и sc-элементу ej, то на с одной стороны, это признак пары ei, ej, а с другой с другой стороны, является моделью (отражением, описанием)

связь либо между денотатом sc-элемента ei и обозначение sc-элемента ej, либо между обозначение sc-элемента ei и самого sc-элемента ej, либо между обозначением sc-элемента ej и самим sc-элементом ei. Если sc-элемент имеет метку sc-узел, то она обозначает сущность, которая не является парой. Если sc-элемент имеет метку sc-вершина, которая инцидентный sc-элементу ei и sc-элементу ej, то представляет собой, с одной стороны, неориентированную пару ei, ei, а с другой стороны, является моделью (отражением, описанием) связь либо между денотатом sc-элемента ei и обозначение sc-элемента ej, либо между обозначение sc-элемента ei и самого sc-элемента ej, либо между обозначением sc-элемента ej и самим sc-элементом ei. Если sc-элемент имеет метку sc-дуги, которая выходит из sc-элемента ei и входит в sc-элемент ej, то на одном с другой стороны, это знакоориентированная пара <ei, ej>, а на с другой стороны, является моделью (отражением, описанием) связь либо между денотатом sc-элемента ei и обозначение sc-элемента ej, либо между обозначение sc-элемента ei и самого sc-элемента ej, либо между обозначением sc-элемента ej и самим sc-элементом ei. Если sc-элемент имеет метку базовой sc-дуги, которая выходит sc-элемент ei и входит в sc-элемент ej, то на одном стороны, является признаком ориентированного постоянного позитивного постоянного парой принадлежности <ei, ej> и, с другой стороны, является модель (отражение, описание) связи между множество, которое обозначается sc-элементом ei и sc-элементом ej, который является одним из элементов указанного множества.]

⇒ *принцип**:

[семантика SC-кода]

⇒ *цитата**:

[Интегральную компьютерную систему можно рассматривать как средство решения проблем, объединяющее несколько моделей проблемы решение и наличие средств взаимодействия с внешняя среда (с другими компьютерными системами, с пользователи)]

⇒ *пояснение**:

[интегральная компьютерная система]

⇒ *цитата**:

[Эпицентром следующего этапа развития информационных технологий станет решение проблемы обеспечения семантической совместимости компьютерных систем и их компонент. Для решения этой проблемы необходимо:

- переход от традиционных компьютерных систем и от современных интеллектуальных систем к семантическим компьютерным системам;
- стандарт разработки семантических компьютерных систем.

]

⇒ *принцип**:

[решение проблемы обеспечения семантической совместимости компьютерных систем и их компонент.]

⇒ *цитата**:

[***Семантический ассоциативный компьютер***

= Аппаратно-реализованный интерпретатор семантики модели (sc-модели) компьютерных систем
= Семантически-ассоциативный компьютер, управляемый знаниями
= Компьютер с нелинейной конструктивно реконструируемой (графодинамической) ассоциативной памятью, обработкой информации, при которой сводится

не к изменению состояния элементов памяти, а изменению конфигурации соединений между ними
= sc-компьютер
= scp-компьютер
= Компьютер управляется знаниями, представленными в SC-код
= Компьютер ориентирован на обработку текстов SC-кода

]

⇒ *пояснение**:

[Семантический ассоциативный компьютер]

Абдурахман Д.Д.ИскусИиМОвК-2022ст

⇒ *ключевой знак**:

- *искусственный интеллект;*
- *кибербезопасность;*
- *машинное обучение*

⇒ *тип источника**:

[статья]

⇒ *аннотация**:

[За последние десятилетия количество кибератак не только значительно увеличилось, но и стало более изощренным. Следовательно, разработка киберустойчивого подхода имеет первостепенное значение. Традиционные методы безопасности недостаточны для предотвращения утечки данных в случае кибератак. Киберпреступники научились использовать новые методы и надежные инструменты для взлома, атаки и взлома данных. К счастью, технологии искусственного интеллекта (AI) были внедрены в киберпространство для создания интеллектуальных моделей защиты систем от атак. Поскольку технологии искусственного интеллекта могут быстро развиваться для решения сложных ситуаций, их можно использовать в качестве основных инструментов в области кибербезопасности. Методы на основе искусственного интеллекта могут предоставить эффективные и мощные инструменты киберзащиты для распознавания атак вредоносного ПО, сетевых вторжений, фишинга и спама, а также утечки данных и оповещения об инцидентах безопасности, когда они происходят. В этой статье мы рассматриваем влияние ИИ на кибербезопасность и обобщаем существующие исследования с точки зрения преимуществ ИИ в кибербезопасности.]

⇒ *цитата**:

[Искусственный интеллект (AI) — чрезвычайно широкая и туманная область, охватывающая множество методологий, в рамках которых машинное обучение можно рассматривать как подмножество или средство достижения ИИ. Большая часть новых разработок и инвестиций в области ИИ посвящена машинному обучению]

⇒ *пояснение**:

[искусственный интеллект]

⇒ *цитата**:

[Машинное обучение — это в основном технология прогнозирования, и многие из его задач можно отнести к нескольким общим категориям, представленным в таблице ниже.]

⇒ *пояснение**:

[машинное обучение]

Баранович А.Е.СеманАИБКЗ-2011ст

⇒ *ключевой знак**:

- *аксиология;*
- *знания;*
- *знаний концентрация;*
- *интеллектуальные системы;*
- *избыточность информации;*
- *информационная безопасность;*
- *семантика;*
- *семантические фильтры;*
- *телеология;*
- *угрозы безопасности*

⇒ *тип источника**:

[статья]

⇒ *аннотация**:

[Статья продолжает цикл работ посвященных семантико-прагматическим аспектам обеспечения информационной безопасности]

⇒ *цитата**:

[Под характеристическим атрибутом И., именуемым в настоящей терминологической системе семантикой (И.), в вербальном контексте обычно понимают интегральную совокупность ее смысла и значения17, возможно и содержания.]

⇒ *пояснение**:

[характеристические атрибуты]

⇒ *цитата**:

[В рамках используемого подхода *объективная семантика* И. характеризует информационные формы существования МС ОР и взаимосвязана с формой, структурой и организацией МС. Соответственно, в модельной интерпретации речь идет о некоторой универсальной структурной ("структуралистической") модели информации МС. В данном контексте любые МС тождественной массы (на уровне "^{2}4 модели мира") различаются структурной организацией (массы кварков), т. е. информацией (ее семантикой – "содержанием").]

⇒ *принцип**:

[объективная семнатика]

⇒ *цитата**:

[В свою очередь, *семантика субъективная* (прагматическая) интерпретируется в рамках ИЭП как динамический информационный образ объективной семантики (информации МС "внешнего мира"), инициализированный в подсистеме знаний воспринимающей ИС.]

⇒ *принцип**:

[семантика субъективная]

⇒ *цитата**:

[В рамках используемого подхода *объективная семантика* И. характеризует информационные формы существования МС ОР и взаимосвязана с формой, структурой и организацией МС. Соответственно, в модельной интерпретации речь идет о некоторой универсальной структурной («структуралистической») модели информации МС. В данном контексте любые МС тождественной массы (на уровне "^{2}4 модели мира") различаются структурной организацией (массы кварков), т. е. информацией (ее семантикой – "содержанием").

В свою очередь, *семантика субъективная* (прагматическая) интерпретируется в

рамках ИЭП как динамический информационный образ объективной семантики (информации МС "внешнего мира"), инициализированный в подсистеме знаний воспринимающей ИС.]

⇐ *сравнение**:

{• *объективная семантика;*
• *субъективная семантика*
}

⇒ *цитата**:

[В феноменологической основе подхода задействованы следующие прагматические свойства И.

1. *Избыточность* И, отражающая уровень превышения необходимого (минимально полного) для использования объема И. В понятие объема И. вкладываются как объективные характеристики количества И. (например, по К. Шеннону), так и ее субъективно-прагматические параметры, отражающие содержательные (семантические) аспекты И.
2. *Краткость* И., характеризующая уровень сокращения объема используемой И. в отношении некоторой вполне определенной реперной единицы. В этом смысле краткость И. есть антоним ее избыточности
3. *Кумулятивность* И., отражающая особенности эффективного функционирования индивидуальных и коллективных систем знаний АИС и заключающаяся в использовании в практической деятельности (семантической коммуникации) кратких (сжатых) форм представления И. При этом полную (в рамках ограничений системы знаний) И. о конкретном явлении можно восстановить (при выполнении условий целостности и доступности) по ее краткой форме представления. В частности, доказанное ранее утверждение на практике можно использовать без доказательства. При вербальном представлении (номинации) знаний свойство кумулятивности И. реализуется путем категориальной свертки понятий, основанной на систематизации и классификации [3]
4. *Рассеиваемость* И. Социальная информация способна рассредоточиваться по различным источникам. Одна и та же информация может быть представлена в различной форме в газете, журнале, книге, отчете, СМИ (радиовещание, телевидение) и т.

]

⇒ *принцип**:

["концентрация знаний"]

Частикова В.А..МетодПСАИ-2022ст

⇒ *ключевой знак**:

- *система анализа инцидентов;*
- *нейроиммунный подход;*
- *событие безопасности;*
- *корреляция;*
- *система правил;*
- *модифицированный генетический алгоритм дуэлей;*
- *глубокое обучение;*
- *искусственная иммунная система*

⇒ *тип источника**:

[статья]

⇒ *аннотация**:

[Предложена методика построения нейроиммунной системы анализа инцидентов информационной безопасности (ИБ), объединяющей модули сбора и хранения (сжатия) данных, модуль анализа и корреляции событий ИБ и подсистемы обнаружения сетевых атак. Особенностью данной системы является применение разработанных методов на основе нейроиммунного подхода, обеспечивающих решение каждой из задач перечисленных модулей. Нейроиммунные методы сжатия данных, обнаружения вторжений, анализа и корреляции инцидентов ИБ объединяют такие интеллектуальные решения, как сверточные нейронные сети, система, основанная на правилах, гибридная искусственная система. Разработан программный комплекс системы анализа инцидентов безопасности. Проведена оценка эффективности предложенного подхода. Показана эффективность работы комплекса в рамках задачи анализа инцидентов ИБ.]

⇒ *цитата**:

[В качестве глубоких нейронных сетей применяются архитектуры сверточных сетей [6]. В качестве ИС используется гибридная искусственная иммунная система (ГИС), объединяющая классический клональный вариант ИС и модифицированный генетический метод дуэлей, основные положения которых описаны в [7].]

⇒ *принцип**:

[архитектура глубоких нейронных сетей]

⇒ *цитата**:

[Общий принцип работы системы анализа инцидентов ИБ, обнаружения вторжений на базе нейроиммунного подхода представляется следующим образом. Для обучения нейроиммунных систем формируется репрезентативная выборка известных инцидентов ИБ, образов сетевых атак, которые предоставляются системе защиты для формирования базы антител – распознавателей опасных объектов, исчерпывающе описывающих каждый из заданных типов атак в случае обнаружения вторжений или корреляционных связей между событиями, составляющими инциденты. Затем обученная нейроиммунная система вводится в узлах в режиме распознавания. При возникновении угрозы в анализируемой сети формируется уведомление об обнаруженной проблеме, поступающее администратору, записывается соответствующий лог.]

⇒ *принцип**:

[работа сисетмы анализа инцидентов ИБ]

⇒ *цитата**:

[Основной функцией системы анализа инцидентов информационной безопасности (САИБ) является анализ и корреляция событий ИБ. Система осуществляет мониторинг сетевой инфраструктуры, получает логи, журналы событий с различных устройств компьютерной сети, формализует полученные сведения, проводит их обработку и представление, что позволяет сформировать описание активности в информационной системе, обеспечивая эффективное решение задачи мониторинга путем выявления отклонений заданных признаков по выбранным критериям]

⇒ *принцип**:

[сиситема анализа]

4 ПРЕДЛОЖЕНИЯ ПО РАЗВИТИЮ ТЕКУЩЕЙ ВЕРСИИ СТАНДАРТА ИНТЕЛЛЕКТУАЛЬНЫХ КОМПЬТЕРНЫХ СИСТЕМ И ТЕХНОЛОГИЙ ИХ РАЗРАБОТКИ

⇒ *предложение**:

[Иерархический коллектив кибернетических систем должен иметь секционированную память("sharding"), так как это повышает ее производительность, так как использование общей памяти и подразумевает то, что модуль, отвечающий за нее будет перегружаться.]

⇒ *предложение**:

[Информация, хранящаяся для отдельных кибернетических систем должна быть сокрыта от других систем, так как это повышает независимость систем, а следствие, что память, отвечающая за каждую систему, не будет перегружаться и будет взаимодействовать с памятью других кибернетических систем в меньшей степени, что снижает количество операций для достижения поставленной цели.]

⇒ *предложение**:

[Аппарат, отвечающий за выполнение простейших операций может иметь двоичную структуру, однако, для большей гибкости, можно использовать структуру с большим основанием.]

⇒ *предложение**:

[Процессор должен поддерживать возможность параллельных вычислений, так как линейное выполнение не приводит к повышению эффективности системы. Для этого он должен иметь многоядерную структуру.]

⇒ *предложение**:

[Для выполнения операций, непосредственно приводящих к развитию системы, следует применять теоретико-категорные методы.]

⇒ *предложение**:

[Для взаимодействия различных кибернетических систем следует применять отдельные агенты, ответственные за их взаимодействие. Это приводит к простоте параллелизуемости и эффективности использования памяти.]

⇒ *предложение**:

[Для организации sc-ребер следует их организовывать в двусвязный список для быстроты доступа к вершинам, а также их добавления(удаления).]

⇒ *предложение**:

[Для эффективного создания шаблонов кибернетических систем следует применять абстрактные классы. Может применятся шаблон "Bridge".]

⇒ *предложение**:

[Как дополнение к прошлому предложению предлагается применять шаблоны "Prototype", "Strategy", "Factory", "Abstract Factory", "Builder", "Singleton"(следует отличать от "Prototype"), а также "Mediator".]

⇒ *предложение**:

[При совместимости различных кибернетических систем может быть использован шаблон "Adapter".]

⇒ *предложение**:

[Понимая, что реализация написана на C++, осмелюсь предложить использование GraphQL, так как многие языки, к примеру, Java, Python, JS имеют возможность их обработки при подключении отдельных фреймворков, а также этот язык запросов имеет несколько особенностей: может быть собран в JSON файл, клиенты могут запросить вложенные поля с помощью единого запроса, что снижает риск перегрузки и недозагрузки, клиенты могут узнать о схеме GraphQL посредством интроспекции, GraphQL достигает сильной типизации с помощью SDL. Однако, как хорошая альтернатива, может быть использован gRPC.]

⇒ *предложение**:

[Предлагается использование MongoDB как того вида баз данных, что необязательно основывается на реляционности.]

⇒ *предложение**:

[меньше полагаться на ассемблер]

ЗАКЛЮЧЕНИЕ

При выполнении работы все концепции, представленные в главе 7.9. монографии, были рассмотрены.

Были рассмотрены следующие вопросы:

- решение вопроса интеграции компьютерных систем;
- экосистема ОСТИС;
- понятие интеллектуальных систем и технологий;
- обеспечение защиты интеллектуальной системы и технологий. Методы защиты интеллектуальных систем и технологий;
- применение экспертных систем;
- когнитивная психология;
- искусственный интеллект и машинное обучение в кибербезопасности;

Кибербезопасность всегда была и всегда будет важной темой в современной технологической среде, поэтому очень важно обеспечить безопасность наших данных и систем, которые их обрабатывают. Системы безопасности в настоящее время не идеальны, поэтому в наших целях обеспечить их работоспособность в лучшем виде.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

[1] Golenkov, V. Methods and tools for ensuring compatibility of computer systems / V. Golenkov. — Open Semantic Technologies for Intelligent Systems (OSTIS-2019), 2019. — P. 25 – 52.

[2] Абдурахман, Д. Д. Искусственный интеллект и машинное обучение в кибербезопасности / Д. Д. Абдурахман. — Современные проблемы лингвистики и методики преподавания русского языка в вузе и школе, 2022. — P. 916–921.

[3] Баранович, А. Е. Семантические аспекты информационной безопасности: концентрация знаний / А. Е. Баранович. — История и архивы, 2011. — P. 38–58.

[4] В. А. Частикова, А. И. Митюгов. Методика построения системы анализа инцидентов информационной безопасности на основе нейроиммунного подхода / А. И. Митюгов В. А. Частикова. — Электронный Сетевой Политематический Журнал «Научные Труды Кубгту», 2022. — P. 98–105.

[5] В.В.Голенков,. Семантические технологии проектирования интеллектуальных систем и семантические ассоциативные компьютеры / В.В.Голенков. — Доклады Белорусского Государственного Университета Информатики И Радиоэлектроники, 2019. — P. 42–50.

[6] В.Н. Дружинина, Д.В. Ушакова. Когнитивная психология. Учебник для вузов / Д.В. Ушакова В.Н. Дружинина. — https://platona.net, 2002. — P. 480.

[7] Дементьев, А. В. Метрики семантических данных / А. В. Дементьев. — Молодой ученый., 2022. — P. 48–51.

[8] К. В. Хоанг, А. Ф. Тузовский. Решения основных задач в разработке программы поддержки безопасности работы с семантическими базами данных / А. Ф. Тузовский К. В. Хоанг. — Доклады ТУСУРа, 2013. — P. 121–125.

[9] Остроух, А. В. Интеллектуальные системы: монография / А. В. Остроух. — Красноярск : Научно-инновационный центр, 2020. — P. 316.

[10] Скрыпников, А. В. Реализация функций информационной безопастности на базе сервисов инфраструктуры OPEN GRID SERVICES ARCHITECTURE / А. В. Скрыпников. — https://cyberleninka.ru, 2011. — P. 82–86.

[11] Созинова, Е. Н. Применение экспертных систем для анализа и оценки информационной безопасности / Е. Н. Созинова. — Молодой ученый, 2011. — P. 64–66.

[12] Ш. И. Исобоев Д. А. Везарко, А. С. Чечельницкий. Интеллектуальная система мониторинга безопасности сети беспроводной связи на основе машинного обучения / А. С. Чечельницкий Ш. И. Исобоев, Д. А. Везарко. — Экономика и качество систем связи, 2022. — Р. 44–48.