

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ

по дисциплине

**«ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ АНАЛИЗА ПРОТОКОЛОВ
БЕЗОПАСНОСТИ»**

для студентов направления подготовки 02.04.01 Математика и компьютерные
науки

профиль "Искусственный интеллект в кибербезопасности"

**Ставрополь
2026**

СОДЕРЖАНИЕ

ВВЕДЕНИЕ	3
СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ	5
Практическое занятие 1. Введение в вероятностные модели" для студентов по предмету.	5
Практическое занятие 2. Пример модели протокола.	6
Практическое занятие 3. Применение вероятностных моделей.	8
Практическое занятие 4. Анализ свойств протоколов.	10
Практическое занятие 5. Построение общего языка для описания свойств.	12
Практическое занятие 6. Вероятностные системы переходов.	14
Практическое занятие 7. Введение в вероятностные системы.	16
Практическое занятие 8. Примеры вероятностных систем.	18
Практическое занятие 9. Выражение свойств вероятностных систем.	20
Практическое занятие 10. Введение в логику ветвящегося времени.	22
Практическое занятие 11. Случайное блуждание и формулы.	24
Практическое занятие 12. Атомарные утверждения и булевы комбинации.	26
Практическое занятие 13. Определение вероятностных формул.	28
Практическое занятие 14. Преобразование требований на естественном языке в формальную запись.	30
Практическое занятие 15. Задача проверки истинности свойств.	32
1.	35
2.	36
3.	37
4.	38
5. Порядок выполнения самостоятельной работы студентом	39
5.1. Методические рекомендации по работе с учебной литературой	39
6.	42

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Интеллектуальные методы анализа протоколов безопасности» является формирование у будущего специалиста по направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» навыков и знаний в области формального анализа и оценки безопасности протоколов обмена информацией. Это включает в себя:

- Понимание основ вероятностных моделей, логических формализмов и других интеллектуальных методов, применяемых для анализа протоколов безопасности.
- Формирование практических навыков по использованию инструментов формальной верификации, таких как SPIN и PRISM, для проверки свойств протоколов.
- Развитие способности выявлять и оценивать потенциальные уязвимости в протоколах безопасности с помощью интеллектуальных методов анализа.
- Освоение методов прогнозирования и предотвращения угроз информационной безопасности с помощью искусственного интеллекта и машинного обучения.

Перечень осваиваемых компетенций:

Код	Формулировка
ПК-8	Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники

Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы высшего образования

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-8 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и	ИД-1 с помощью современных информационных технологий, исследует вновь создаваемые математические модели в естественных науках промышленности.	знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом

бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники		возможностей современных информационных технологий, программирования и компьютерной техники
ПК-8 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	ИД-2 Проводит Параллельные компьютерные и сетевые технологии в рамках профессиональной деятельности	умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники
ПК-8 Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники	ИД-3 Использует современные языки программирования и пакеты прикладных программ для реализации конкретных алгоритмов и математических моделей	владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1. Введение в вероятностные модели" для студентов по предмету.

Цель работы:

- Научиться применять вероятностные модели для анализа безопасности протоколов.
- Освоить навыки построения и анализа вероятностных моделей в контексте информационной безопасности.

Задание:

1. Построение вероятностной модели атаки на протокол безопасности:

- Выберите один из распространенных протоколов безопасности (например, SSL/TLS).
- Опишите возможные сценарии атак на этот протокол (например, перехват данных, подделка сертификатов).
- Постройте вероятностную модель, которая описывает вероятность успеха атаки в зависимости от различных факторов (например, мощности вычислительных ресурсов, качества криптографии).

2. Анализ модели:

- Вычислите вероятность успеха атаки при различных условиях (например, при использовании слабых паролей, при наличии уязвимостей в реализации).
- Проанализируйте, как изменения в параметрах модели (например, увеличение вычислительной мощности) влияют на вероятность успеха атаки.

3. Реализация модели:

- Используя программные инструменты (например, Python с библиотеками NumPy и SciPy), реализуйте построенную модель и проведите симуляции для оценки вероятности успеха атаки при различных сценариях.

4. Выводы и рекомендации:

- На основе результатов симуляций сформулируйте рекомендации по повышению безопасности протокола (например, использование более сильных криптографических алгоритмов, регулярные обновления программного обеспечения).

Контрольные вопросы:

1. Какие типы атак на протоколы безопасности можно описать с помощью вероятностных моделей?
2. Как вероятностные модели могут помочь в оценке рисков информационной безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа вероятностных моделей в информационной безопасности?

Перечень основной литературы

1. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002)2.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015)3.
3. Ивченко Г.И., Медведев Ю.И. "Дискретные вероятностные модели" (URSS.ru).

Перечень дополнительной литературы

1. Матвеев С.А. "Вероятностная модель надежности реализации в автоматизированных системах функций защиты информации от несанкционированного доступа" (Военно-космическая академия имени А. Ф. Можайского)2.
2. Статья "Вероятностная модель оценки информационного воздействия" (КиберЛенинка)5.
3. Учебное пособие "Основы информационной безопасности" (УрФУ)6.
4. Статья "Теоретико-вероятностная модель оценки рисков информационной безопасности предприятия" (КиберЛенинка)

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnik.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование
<http://www.myersbriggs.org> <http://keirseey.com>

Практическое занятие 2. Пример модели протокола.

Цель работы:

- Научиться анализировать и моделировать протоколы безопасности.
- Освоить навыки построения и анализа моделей протоколов в контексте информационной безопасности.

Задание:

1. **Выбор протокола безопасности:**
 - Выберите один из известных протоколов безопасности, например, протокол Needham-Schroeder (NS) для взаимной аутентификации¹.
2. **Описание протокола:**
 - Опишите шаги протокола и его цель (например, аутентификация, шифрование данных).
 - Объясните, какие криптографические примитивы используются в протоколе (например, симметричное или асимметричное шифрование).
3. **Анализ безопасности:**
 - Проанализируйте потенциальные уязвимости протокола (например, атаки "человек посередине", утечки данных).
 - Оцените эффективность протокола в различных сценариях (например, при наличии сильных или слабых паролей).
4. **Модификация протокола:**
 - Предложите модификации протокола для повышения его безопасности (например, использование более сильных криптографических алгоритмов).
 - Объясните, как эти модификации влияют на производительность и безопасность протокола.

Контрольные вопросы:

1. Какие основные криптографические примитивы используются в протоколах безопасности?
2. Как можно улучшить безопасность протоколов путем модификации их шагов или используемых алгоритмов?
3. Какие сетевые модели (например, OSI) можно использовать для анализа протоколов безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Протоколы защиты на канальном и сеансовом уровнях" (YZTM.RU) — Описание сетевых протоколов безопасности в модели OSI.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Еще раз о важности построения модели противника" (RusCrypto) — Анализ безопасности протоколов с точки зрения модели противника.
4. Список сетевых протоколов (Wikipedia) — Обзор различных сетевых протоколов, используемых на разных уровнях модели OS

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 3. Применение вероятностных моделей.

Цель работы:

- Научиться применять вероятностные модели для анализа безопасности протоколов.
- Освоить навыки построения и анализа вероятностных моделей в контексте информационной безопасности.

Задание:

1. Выбор протокола безопасности:

- Выберите один из известных протоколов безопасности, например, протокол SSL/TLS.
- Опишите основные шаги протокола и его цель (например, шифрование данных, аутентификация).

2. Построение вероятностной модели:

- Постройте вероятностную модель, которая описывает вероятность успеха атаки на выбранный протокол в зависимости от различных факторов (например, мощности вычислительных ресурсов, качества криптографии).
- Используйте игровую модель или модель с полным перекрытием для анализа потенциальных угроз и защиты.

3. Анализ модели:

- Вычислите вероятность успеха атаки при различных условиях (например, при использовании слабых паролей, при наличии уязвимостей в реализации).
- Проанализируйте, как изменения в параметрах модели (например, увеличение вычислительной мощности) влияют на вероятность успеха атаки.

4. Реализация модели:

- Используя программные инструменты (например, Python с библиотеками NumPy и SciPy), реализуйте построенную модель и проведите симуляции для оценки вероятности успеха атаки при различных сценариях.

5. Выводы и рекомендации:

- На основе результатов симуляций сформулируйте рекомендации по повышению безопасности протокола (например, использование более сильных криптографических алгоритмов, регулярные обновления программного обеспечения).

Контрольные вопросы:

1. Какие типы атак на протоколы безопасности можно описать с помощью вероятностных моделей?
2. Как вероятностные модели могут помочь в оценке рисков информационной безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа вероятностных моделей в информационной безопасности?

Перечень основной литературы

1. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности.

Перечень дополнительной литературы

1. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 4. Анализ свойств протоколов.

Цель работы:

- Научиться анализировать свойства протоколов безопасности.
- Освоить навыки оценки и улучшения безопасности протоколов.

Задание:

1. Выбор протокола безопасности:

- Выберите один из известных протоколов безопасности, например, протокол SSL/TLS.
- Опишите основные шаги протокола и его цель (например, шифрование данных, аутентификация).

2. Анализ свойств безопасности:

- Оцените свойства безопасности протокола, такие как:
 - Целостность сообщений: Способность обнаруживать изменения в сообщениях во время передачи.
 - Секретность: Защита от неавторизованного доступа к передаваемой информации.
 - Аутентификация: Способность подтвердить личность участников обмена.
- Проанализируйте, как протокол обеспечивает эти свойства с помощью криптографических примитивов (например, симметричное или асимметричное шифрование, хэш-функции).

3. Оценка уязвимостей:

- Опишите возможные уязвимости протокола (например, атаки "человек посередине", утечки данных).
- Проанализируйте, как эти уязвимости могут быть использованы противниками для нарушения свойств безопасности.

4. Улучшение безопасности:

- Предложите модификации протокола для повышения его безопасности (например, использование более сильных криптографических алгоритмов).
- Объясните, как эти модификации влияют на производительность и безопасность протокола.

Контрольные вопросы:

1. Какие основные свойства безопасности должны обеспечивать протоколы безопасности?
2. Как можно улучшить безопасность протоколов путем модификации их шагов или используемых алгоритмов?
3. Какие сетевые модели (например, OSI) можно использовать для анализа протоколов безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Исследование протоколов сетевой безопасности" (CyberLeninka.ru) — Анализ протоколов SSL/TLS, SSH и других⁴.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Сетевые протоколы нового поколения и их анализ с точки зрения информационной безопасности" (CyberLeninka.ru) — Обзор протоколов HTTP/2, QUIC и HTTP/3⁷.
4. Документ "Уязвимости протоколов безопасности" (Teach-in.ru) — Описание классов противников и их возможностей

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 5. Построение общего языка для описания свойств.

Цель работы:

- Научиться разрабатывать общий язык для описания свойств безопасности протоколов.
- Освоить навыки формализации и стандартизации описаний свойств безопасности.

Задание:

1. Изучение существующих подходов:

- Ознакомьтесь с существующими языками и стандартами для описания свойств безопасности, такими как CWE (Common Weakness Enumeration) и OWASP (Open Web Application Security Project).
- Проанализируйте их сильные и слабые стороны в контексте описания свойств безопасности протоколов.

2. Определение ключевых свойств:

- Определите основные свойства безопасности, которые должны быть включены в общий язык, такие как:
 - **Аутентификация**
 - **Целостность**
 - **Секретность**
 - **Доступность**
 - **Неотказуемость.**

3. Разработка языка:

- Разработайте структуру и синтаксис общего языка для описания свойств безопасности протоколов.
- Обеспечьте, чтобы язык был простым, гибким и расширяемым для описания различных протоколов и сценариев.

4. Применение языка:

- Примените разработанный язык для описания свойств конкретного протокола безопасности (например, SSL/TLS).
- Оцените эффективность языка в описании свойств безопасности и выявлении потенциальных уязвимостей.

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование
5. <https://urait.ru/bcode/449575> – Зенкина, С. В. Сетевая проектно-исследовательская деятельность обучающихся : учебное пособие для вузов / С. В. Зенкина, Е. К. Герасимова, О. П. Панкратова. — Москва : Издательство Юрайт, 2020. — 152 с. — (Высшее образование). — ISBN 978-5-534-13229-8. — Текст : электронный // ЭБС Юрайт [сайт].

Практическое занятие 6. Вероятностные системы переходов.

Цель работы:

- **Научиться** использовать вероятностные системы переходов для анализа протоколов безопасности.
- **Освоить** навыки моделирования и анализа вероятностных свойств протоколов.

Задание:

1. **Выбор протокола безопасности:**
 - Выберите один из известных протоколов безопасности, например, протокол SSL/TLS.
 - Опишите основные шаги протокола и его цель (например, шифрование данных, аутентификация).
2. **Построение вероятностной системы переходов:**
 - Постройте вероятностную систему переходов, которая описывает поведение протокола в различных состояниях (например, успешная аутентификация, обнаружение атаки).
 - Используйте инструменты, такие как PRISM, для моделирования и анализа вероятностных свойств протокола.
3. **Анализ вероятностных свойств:**
 - Вычислите вероятность успеха атаки на протокол при различных условиях (например, при использовании слабых паролей, при наличии уязвимостей в реализации).
 - Проанализируйте, как изменения в параметрах модели (например, увеличение вычислительной мощности) влияют на вероятность успеха атаки.
4. **Реализация модели:**
 - Используя программные инструменты (например, PRISM), реализуйте построенную модель и проведите симуляции для оценки вероятности успеха атаки при различных сценариях.
5. **Выводы и рекомендации:**
 - На основе результатов симуляций сформулируйте рекомендации по повышению безопасности протокола (например, использование более сильных криптографических алгоритмов, регулярные обновления программного обеспечения).

Контрольные вопросы:

1. Какие типы атак на протоколы безопасности можно описать с помощью вероятностных систем переходов?
2. Как вероятностные системы переходов могут помочь в оценке рисков информационной безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа вероятностных систем переходов в информационной безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁶.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Методика оценки безопасности криптографических протоколов" (CyberLeninka.ru) — Применение теории «доказуемой стойкости» для оценки безопасности протоколов³.
4. Документ "Методы верификации программ" (MSU) — Обзор методов верификации программ, которые могут быть применены к протоколам безопасности⁷.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 7. Введение в вероятностные системы.

Цель работы:

- **Научиться** понимать основы вероятностных систем и их применение в анализе протоколов безопасности.
- **Освоить** навыки построения и анализа вероятностных моделей в контексте информационной безопасности.

Задание:

1. Изучение основ вероятностных систем:

- Ознакомьтесь с основными понятиями теории вероятностей, такими как вероятностное пространство, случайные события и их вероятности.
- Поймите различия между классическим, геометрическим и статистическим определениями вероятности.

2. Применение вероятностных систем в безопасности:

- Выберите один из протоколов безопасности (например, SSL/TLS) и опишите, как вероятностные системы могут быть использованы для анализа его безопасности.
- Рассмотрите примеры вероятностных моделей, которые могут быть применены для оценки рисков и уязвимостей в протоколе (например, вероятность успеха атаки "человек посередине").

3. Построение простой вероятностной модели:

- Постройте простую вероятностную модель для описания вероятности успеха атаки на выбранный протокол.
- Используйте инструменты, такие как Python с библиотеками NumPy и SciPy, для реализации и симуляции модели.

4. Анализ и выводы:

- Проанализируйте результаты симуляций и сформулируйте рекомендации по повышению безопасности протокола на основе вероятностного анализа.

Контрольные вопросы:

1. Какие основные понятия теории вероятностей используются в анализе протоколов безопасности?
2. Как вероятностные системы могут помочь в оценке рисков информационной безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа вероятностных систем в информационной безопасности?

Перечень основной литературы

1. Агеев В.В., Тихов М.С. "Введение в теорию вероятностей" (Н.Новгород, 2012) — Учебно-методическое пособие по теории вероятностей¹.
2. Лекции по теории вероятностей и математической статистике (ТПУ) — Обзор теоретических понятий и определений теории вероятностей².
3. Учебное пособие "Основы теории вероятностей" (МГУ) — Основные положения теории вероятностей и математической статистики⁴.

Перечень дополнительной литературы

1. Агеев В.В., Тихов М.С. "Введение в теорию вероятностей" (Н.Новгород, 2012) — Учебно-методическое пособие по теории вероятностей¹.
2. Лекции по теории вероятностей и математической статистике (ТПУ) — Обзор теоретических понятий и определений теории вероятностей².
3. Учебное пособие "Основы теории вероятностей" (МГУ) — Основные положения теории вероятностей и математической статистики⁴.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 8. Примеры вероятностных систем.

Цель работы:

- **Научиться** понимать и применять вероятностные системы для анализа протоколов безопасности.
- **Освоить** навыки построения и анализа вероятностных моделей в контексте информационной безопасности.

Задание:

1. Изучение примеров вероятностных систем:

- Ознакомьтесь с примерами вероятностных систем переходов, такими как упрощенная модель протокола передачи сообщений через ненадежный канал.
- Проанализируйте, как вероятностные системы могут быть использованы для оценки безопасности протоколов обмена ключами.

2. Построение вероятностной модели:

- Выберите один из протоколов безопасности (например, протокол Needham-Schroeder) и постройте вероятностную модель, которая описывает вероятность успеха атаки на этот протокол.
- Используйте инструменты, такие как PRISM, для моделирования и анализа вероятностных свойств протокола.

3. Анализ и выводы:

- Вычислите вероятность успеха атаки при различных условиях (например, при использовании слабых паролей, при наличии уязвимостей в реализации).
- Проанализируйте, как изменения в параметрах модели (например, увеличение вычислительной мощности) влияют на вероятность успеха атаки.

4. Реализация модели:

- Используя программные инструменты (например, Python с библиотеками NumPy и SciPy), реализуйте построенную модель и проведите симуляции для оценки вероятности успеха атаки при различных сценариях.

5. Выводы и рекомендации:

- На основе результатов симуляций сформулируйте рекомендации по повышению безопасности протокола (например, использование более сильных криптографических алгоритмов, регулярные обновления программного обеспечения).

Контрольные вопросы:

1. Какие типы атак на протоколы безопасности можно описать с помощью вероятностных систем?
2. Как вероятностные системы могут помочь в оценке рисков информационной безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа вероятностных систем в информационной безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.

2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁴.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасности⁶.
4. Документ "Вероятностный анализ безопасности" (Gosatomnadzor.mchs.gov.by) — Описание целей и объема вероятностного анализа безопасности.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 9. Выражение свойств вероятностных систем.

Цель работы:

- **Научиться** выражать свойства вероятностных систем в контексте анализа протоколов безопасности.
- **Освоить** навыки формализации и анализа вероятностных свойств протоколов.

Задание:

1. Изучение свойств вероятностных систем:

- Ознакомьтесь с основными свойствами вероятностных систем, такими как независимость событий, условная вероятность и теорема Байеса.
- Проанализируйте, как эти свойства могут быть применены для анализа безопасности протоколов.

2. Выбор протокола безопасности:

- Выберите один из известных протоколов безопасности, например, протокол SSL/TLS.
- Опишите основные шаги протокола и его цель (например, шифрование данных, аутентификация).

3. Выражение свойств вероятностных систем:

- Выразите вероятностные свойства протокола с помощью математических формул и уравнений.
- Используйте понятия теории вероятностей, такие как вероятность успеха атаки, вероятность обнаружения ошибок, для описания свойств протокола.

4. Анализ и выводы:

- Проанализируйте, как изменения в параметрах вероятностной системы (например, увеличение вычислительной мощности) влияют на свойства безопасности протокола.
- Сделайте выводы о том, как вероятностные системы могут помочь в оценке и улучшении безопасности протоколов.

Контрольные вопросы:

1. Какие основные свойства вероятностных систем используются в анализе протоколов безопасности?
2. Как вероятностные системы могут помочь в оценке рисков информационной безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа вероятностных систем в информационной безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁴.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасности⁶.

4. Документ "Вероятностный анализ безопасности" (Gosatomnadzor.mchs.gov.by) — Описание целей и объема вероятностного анализа безопасности.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnik.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 10. Введение в логику ветвящегося времени.

Цель работы:

- **Научиться** понимать основы логики ветвящегося времени и ее применение в анализе протоколов безопасности.
- **Освоить** навыки использования логики ветвящегося времени для формализации и анализа свойств протоколов.

Задание:

1. Изучение основ логики ветвящегося времени:

- Ознакомьтесь с основными понятиями логики ветвящегося времени, такими как CTL (Computation Tree Logic) и ее операторы (например, AX, EX, AF, EF).
- Поймите, как эти операторы используются для описания свойств вычислительных систем.

2. Применение логики ветвящегося времени к протоколам безопасности:

- Выберите один из протоколов безопасности (например, SSL/TLS) и опишите, как логику ветвящегося времени можно использовать для анализа его свойств.
- Примеры свойств: "Всегда выполняется аутентификация перед передачей данных" или "Существует путь, на котором аутентификация не требуется".

3. Формализация свойств с помощью CTL:

- Напишите CTL-формулы для описания выбранных свойств протокола.
- Объясните, как эти формулы могут быть использованы для проверки корректности протокола с помощью инструментов верификации.

4. Анализ и выводы:

- Проанализируйте, как использование логики ветвящегося времени может помочь в выявлении потенциальных уязвимостей протокола.
- Сделайте выводы о том, как CTL может быть применена для улучшения безопасности протоколов.

Контрольные вопросы:

1. Какие основные операторы используются в логике ветвящегося времени CTL?
2. Как CTL может помочь в анализе протоколов безопасности?
3. Какие инструменты и методы можно использовать для верификации CTL-формул в контексте протоколов безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁴.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасности⁶.
4. Документ "Вероятностный анализ безопасности" (Gosatomnadzor.mchs.gov.by) — Описание целей и объема вероятностного анализа безопасности.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 11. Случайное блуждание и формулы.

Цель работы:

- **Научиться** понимать основы случайного блуждания и его применение в анализе протоколов безопасности.
- **Освоить** навыки использования формул и моделей случайного блуждания для оценки свойств протоколов.

Задание:

1. Изучение основ случайного блуждания:

- Ознакомьтесь с понятием случайного блуждания и его типами (например, одномерное случайное блуждание по числовой прямой).
- Поймите, как случайное блуждание может быть использовано для моделирования поведения протоколов безопасности в различных сценариях.

2. Применение формул случайного блуждания:

- Выберите один из протоколов безопасности (например, протокол передачи данных через ненадежный канал) и опишите, как формулы случайного блуждания могут быть использованы для оценки вероятности успеха атаки или обнаружения ошибок.
- Используйте формулы, такие как ожидаемое количество шагов для достижения определенного состояния или вероятность нахождения в определенном состоянии после n шагов.

3. Моделирование и анализ:

- Используя программные инструменты (например, Python), реализуйте модель случайного блуждания для описания поведения протокола.
- Проведите симуляции для оценки вероятности успеха атаки или обнаружения ошибок при различных условиях (например, при изменении вероятности ошибок в канале).

4. Выводы и рекомендации:

- На основе результатов симуляций сформулируйте рекомендации по повышению безопасности протокола (например, использование более надежных методов обнаружения ошибок).

Контрольные вопросы:

1. Какие основные формулы используются в моделировании случайного блуждания?
2. Как случайное блуждание может помочь в анализе протоколов безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа моделей случайного блуждания в информационной безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁴.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасности⁶.
4. Документ "Вероятностный анализ безопасности" (Gosatomnadzor.mchs.gov.by)

— Описание целей и объема вероятностного анализа безопасности. **Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине**

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 12. Атомарные утверждения и булевы комбинации.

Цель работы:

- **Научиться** понимать и применять атомарные утверждения и булевы комбинации для анализа протоколов безопасности.
- **Освоить** навыки использования булевой логики для формализации и анализа свойств протоколов.

Задание:

1. Изучение атомарных утверждений:

- Ознакомьтесь с понятием атомарных утверждений в логике высказываний и их ролью в формировании составных высказываний.
- Поймите, как атомарные утверждения могут быть использованы для описания базовых свойств протоколов безопасности (например, "Сообщение зашифровано").

2. Применение булевых комбинаций:

- Выберите один из протоколов безопасности (например, SSL/TLS) и опишите, как булевы комбинации могут быть использованы для формализации его свойств.
- Примеры булевых комбинаций: "Сообщение зашифровано И аутентифицировано" или "Сообщение зашифровано ИЛИ аутентифицировано".

3. Формализация свойств с помощью булевой логики:

- Напишите булевы формулы для описания выбранных свойств протокола.
- Объясните, как эти формулы могут быть использованы для проверки корректности протокола с помощью инструментов верификации.

4. Анализ и выводы:

- Проанализируйте, как использование булевой логики может помочь в выявлении потенциальных уязвимостей протокола.
- Сделайте выводы о том, как булева логика может быть применена для улучшения безопасности протоколов.

Контрольные вопросы:

1. Какие основные логические операции используются в булевой логике?
2. Как булева логика может помочь в анализе протоколов безопасности?
3. Какие инструменты и методы можно использовать для верификации булевых формул в контексте протоколов безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁴.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасности⁶.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 13. Определение вероятностных формул.

Цель работы:

- **Научиться** определять и применять вероятностные формулы для анализа протоколов безопасности.
- **Освоить** навыки использования вероятностных моделей для оценки рисков и свойств протоколов.

Задание:

1. Изучение вероятностных формул:

- Ознакомьтесь с основными вероятностными формулами, такими как формула полной вероятности, формула Байеса и формула условной вероятности.
- Поймите, как эти формулы могут быть использованы для анализа протоколов безопасности.

2. Применение вероятностных формул к протоколам безопасности:

- Выберите один из протоколов безопасности (например, SSL/TLS) и опишите, как вероятностные формулы могут быть использованы для оценки вероятности успеха атаки или обнаружения ошибок.
- Используйте формулы для описания свойств протокола, таких как вероятность успешной аутентификации или вероятность перехвата данных.

3. Расчет вероятностей:

- Используя вероятностные формулы, рассчитайте вероятность успеха атаки при различных условиях (например, при использовании слабых паролей, при наличии уязвимостей в реализации).
- Проанализируйте, как изменения в параметрах модели (например, увеличение вычислительной мощности) влияют на вероятность успеха атаки.

4. Реализация модели:

- Используя программные инструменты (например, Python с библиотеками NumPy и SciPy), реализуйте построенную модель и проведите симуляции для оценки вероятности успеха атаки при различных сценариях.

5. Выводы и рекомендации:

- На основе результатов симуляций сформулируйте рекомендации по повышению безопасности протокола (например, использование более сильных криптографических алгоритмов, регулярные обновления программного обеспечения).

Контрольные вопросы:

1. Какие основные вероятностные формулы используются в анализе протоколов безопасности?
2. Как вероятностные формулы могут помочь в оценке рисков информационной безопасности?
3. Какие инструменты и методы можно использовать для реализации и анализа вероятностных моделей в информационной безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).

3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов4.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасности6.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
2. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
4. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 14. Преобразование требований на естественном языке в формальную запись.

Цель работы:

- **Научиться** преобразовывать требования безопасности, описанные на естественном языке, в формальную запись.
- **Освоить** навыки использования формальных языков для описания свойств протоколов безопасности.

Задание:

1. Изучение формальных языков:

- Ознакомьтесь с основными формальными языками, такими как логика высказываний и логика предикатов.
- Поймите, как эти языки могут быть использованы для формализации требований безопасности.

2. Преобразование требований:

- Выберите несколько требований безопасности, описанных на естественном языке (например, "Сообщение должно быть зашифровано перед передачей").
- Преобразуйте эти требования в формальную запись с помощью логических формул (например, $\forall x(P(x) \rightarrow Q(x))$ $\forall x(P(x) \rightarrow Q(x))$), где $P(x)$ — "Сообщение передается", а $Q(x)$ — "Сообщение зашифровано").

3. Анализ и проверка:

- Проанализируйте преобразованные формулы на предмет их точности и полноты.
- Проверьте, как эти формулы могут быть использованы для верификации свойств протоколов безопасности с помощью инструментов формальной верификации.

4. Реализация и симуляция:

- Используя программные инструменты (например, Python с библиотеками для логического программирования), реализуйте преобразованные формулы и проведите симуляции для проверки корректности протокола.

Контрольные вопросы:

1. Какие основные формальные языки используются для описания требований безопасности?
2. Как преобразование требований в формальную запись может помочь в анализе протоколов безопасности?
3. Какие инструменты и методы можно использовать для верификации формальных формул в контексте протоколов безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁴.
2. Учебное пособие "Основы информационной безопасности" (УрФУ).

3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасностиб.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

3. Методические указания по организации самостоятельной работы студентов по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.
4. Методические указания к практическим занятиям по дисциплине «Организация командной работы в онлайн среде». Ставрополь : СКФУ, 2021.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

5. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
6. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
7. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
8. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

Практическое занятие 15. Задача проверки истинности свойств.

Цель работы:

- **Научиться** проверять истинность свойств безопасности протоколов с помощью формальных методов.
- **Освоить** навыки использования инструментов формальной верификации для анализа протоколов.

Задание:

1. **Изучение свойств безопасности:**
 - Ознакомьтесь с основными свойствами безопасности, такими как аутентификация, целостность и секретность данных.
 - Поймите, как эти свойства могут быть нарушены в протоколах безопасности.
2. **Выбор протокола безопасности:**
 - Выберите один из известных протоколов безопасности, например, протокол SSL/TLS.
 - Опишите основные шаги протокола и его цель (например, шифрование данных, аутентификация).
3. **Формализация свойств:**
 - Напишите формальные формулы для описания выбранных свойств протокола (например, с помощью логических операторов CTL или LTL).
 - Объясните, как эти формулы могут быть использованы для проверки корректности протокола с помощью инструментов верификации.
4. **Проверка истинности свойств:**
 - Используя программные инструменты (например, SPIN, PRISM), проверьте истинность формализованных свойств для выбранного протокола.
 - Проанализируйте результаты проверки и выявите потенциальные уязвимости или ошибки в протоколе.
5. **Выводы и рекомендации:**
 - На основе результатов проверки сформулируйте рекомендации по улучшению безопасности протокола (например, использование более сильных криптографических алгоритмов).

Контрольные вопросы:

1. Какие основные свойства безопасности должны обеспечивать протоколы безопасности?
2. Как формальные методы могут помочь в проверке истинности свойств протоколов?
3. Какие инструменты и методы можно использовать для верификации свойств в контексте протоколов безопасности?

Перечень основной литературы

1. Миронов А.М. "Протоколы безопасности, часть 1" (MathNet.ru) — Обзор криптографических примитивов и протоколов безопасности¹.
2. Щеглов А.Ю., Щеглов К.А. "Математические модели и методы формального проектирования систем защиты информационных систем" (СПб: Университет ИТМО, 2015).
3. Гаценко О.Ю. "Защита информации: концептуальные и методологические основы защиты информации" (М.: Горячая линия–Телеком, 2002).

Перечень дополнительной литературы

1. Статья "Верификация протоколов безопасности на основе вероятностной проверки" (MathNet.ru) — Использование PRISM для оценки вероятностных свойств протоколов⁴.

2. Учебное пособие "Основы информационной безопасности" (УрФУ).
3. Статья "Применение вероятностных моделей в информационной безопасности" (CyberLeninka.ru) — Описание методологии вероятностного анализа безопасности.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

9. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
10. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
11. <https://spravochnick.ru/psihologiya/> – Справочник по психологии
12. <https://ur-l.ru/LLEbZ> – Тимбилдинг и эффективное командообразование

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

для обучающихся по организации и проведению самостоятельной работы

по дисциплине «ИНТЕЛЛЕКТУАЛЬНЫЕ МЕТОДЫ АНАЛИЗА
ПРОТОКОЛОВ БЕЗОПАСНОСТИ»

для студентов направления подготовки

направленность (профиль):

Ставрополь

2026

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов). Владиславу Вячеславовичу

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

- формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);
- написание докладов;
- подготовка к семинарам, практическим и лабораторным работам, их оформление;
- составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);
- выполнение учебно-исследовательских работ, проектная деятельность;
- подготовка практических разработок и рекомендаций по решению проблемной ситуации;
- выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

- компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

- выполнение курсовых работ (проектов) в рамках дисциплин;

- выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);

- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);

- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационные технологии командной работы и проектной деятельности» направлена на формирование следующих **компетенций**:

Код	Формулировка
ПК-8	Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и универсальных компетенций будущего бакалавра.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоятельной работы	Средства и технологии оценки	Объем часов, в том числе (астр.)		
				СРС	Контактная работа с преподавателем	Всего
3 семестр						
ПК-8	Подготовка к лекциям	Конспект лекций	Собеседование	33,0	18,0	51,0
ПК-8	Подготовка к практическим занятиям	Отчет в электронном виде	Собеседование	33,0	18,0	51,0
ПК-8	Самостоятельное изучение литературы	Конспект	Собеседование	23,0	18,0	41,0
ПК-8	Самотестирование, подготовка к тестированию	Тестирование	Тестовые задания	10,0	18,0	28,0
Итого за 3 семестр				99,0	72,0	171,0
Итого				99,0	72,0	171,0

4. Контрольные точки и виды отчетности по ним

Контроль качества и сроков самостоятельной работы выполняется в соответствии с учебным графиком и оформляется в соответствии с заданием. Предусмотрена следующая рейтинговая оценка знаний

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

5. Порядок выполнения самостоятельной работы студентом

5.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют **четыре основные установки в чтении научного текста:**

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

5.2. Методические рекомендации по составлению конспекта лекций:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.

2. Выделите главное, составьте план.
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

5.3. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Практические работы № 1-5,8 выполняются студентами заочной и очно-заочной формы обучения самостоятельно.

5.4. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Критерии оценки:

Оценка «отлично» выставляется студенту, если он, отлично знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, отлично умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, отлично владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники.

Оценка «хорошо» выставляется студенту, если он, умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники.

Оценка «удовлетворительно» выставляется студенту, если он, плохо знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, плохо умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, плохо владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники.

Оценка «неудовлетворительно» выставляется студенту, если он, не знает как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, не умеет создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники, не владеет как создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий, программирования и компьютерной техники. Компетенция ПК-8 не освоен.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

5.6. Методические рекомендации по подготовке к зачетам

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

6. Список литературы для выполнения СРС

Перечень основной литературы

1. Дзаурова Х. М. и др. Эффективность и безопасность модифицированного протокола кардиоверсии фибрилляции предсердий с использованием отечественного антиаритмического препарата Рефралон. Первые результаты клинического применения // Кардиологический вестник. – 2021. – Т. 16. – №. 1. – С. 49-55.

2. Щеглов А. Ю., Щеглов К. А. Математические модели и методы формального проектирования систем защиты информационных систем. – 2015.
3. Клименко И. С. Информационная безопасность и защита информации: модели и методы управления. – 2020.

Перечень дополнительной литературы

1. Кулик Т. и др. Обзор практических формальных методов обеспечения безопасности //Формальные аспекты вычислительной техники. – 2022. – Т. 34. – №. 1. – С. 1-39.
2. Мендес Д. М., Папапанагиоту И., Янг Б. Интернет вещей: обзор безопасности и конфиденциальности //Препринт arXiv arXiv: 1707.01879. – 2017.
3. Абдул-Гани Х. А., Константас Д. Всестороннее исследование принципов безопасности и конфиденциальности, угроз и контрмер: взгляд на Интернет вещей //Журнал сетей датчиков и исполнительных механизмов. – 2019. – Т. 8. – №. 2. – С. 22.
4. Демилло Р. А., Линч Н. А., Мерритт М. Дж. Криптографические протоколы //Материалы четырнадцатого ежегодного симпозиума АСМ по теории вычислений. – 1982. – С. 383-400.

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Интеллектуальные методы анализа протоколов безопасности». Ставрополь : СКФУ, 2025.
2. Методические указания к практическим занятиям по дисциплине «Интеллектуальные методы анализа протоколов безопасности». Ставрополь : СКФУ, 2025.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. <http://biblioclub.ru/> – Университетская библиотека online "Библиоклуб"
2. <https://4brain.ru/liderstvo/> – Лидерство: уроки эффективного руководителя
3. <https://spravochnik.ru/psihologiya/> – Справочник по психологии