МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«Информационная безопасность открытых систем»

Специальность – 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника – Специалист по защите информации

Специализация – «Безопасность открытых информационных систем»

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем», утвержденного приказом Министерства образования и науки №1509 от 01.12.2016 г.

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):
Доцент, к.ф.-м.н. Д.В.Ильин
старший преподаватель С.О. Иванов

ОБСУЖДЕНО:
на заседании кафедры математического и аппаратного обеспечения информационных систем
«30» августа 2017г., протокол №1

заведующий кафедрой Д.В. Ильин

СОГЛАСОВАНО:

Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., протокол №1

Декан факультета А.В. Щипцова

Директор научной библиотеки Н.Д. Никитина

Начальник управления информатизации И.П. Пивоваров

Начальник учебно-методического управления В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Цель дисциплины: изучение принципов проектирования и анализа защищенности открытых систем.

Основными задачами дисциплины являются:

- изучение архитектур открытых систем;
- проектирование, эксплуатация и совершенствование системы управления информационной безопасностью открытой информационной системы.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Информационная безопасность открытых систем» относится к числу дисциплин базовой части. Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Системное программное обеспечение», «Открытые информационные системы», «Организация ЭВМ и вычислительных систем», «Безопасность операционных систем», «Управление информационной безопасностью», «Основы информационной безопасности», «Организационное и правовое обеспечение информационной безопасности».

Дисциплина является предшествующей для дисциплин: «Безопасность сетей ЭВМ», «Виртуальные частные сети», прохождения производственных и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

– способность создавать и исследовать модели автоматизированных систем (ПК-2);

– способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);

– способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);

– способность разрабатывать и анализировать проектные решения по обеспечению безопасности автоматизированных систем (ПК-8);

– способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);

– способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

– способность на практике применять нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (ПСК-4.1);

– способность разрабатывать и реализовывать политики информационной безопасности открытых информационных систем (ПСК-4.2);

– способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);

– способность участвовать в организации и проведении контроля обеспечения информационной безопасности открытой информационной системы (ПСК-4.4);

– способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5).

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

– модели и фреймворки используемых для описания открытых систем (З1);
– модели угроз и модели нарушителя информационной безопасности автоматизированной системы (З2);
– терминологию и принципы риск-менеджмента (З3);
– международные стандарты и методологии в области проектирования и анализа открытых информационных систем (З4);
– принципы работы средств защиты информационно-технологических ресурсов автоматизированной системы (З5);
– архитектуру информационной безопасности автоматизированной системы (З6);
– нормативные документы, относящиеся к обеспечению информационной безопасности открытых информационных систем (З7);
– принципы разработки политики информационной безопасности открытых информационных систем (З8);
– принципы организации системы управления информационной безопасностью открытой информационной системы (З9);
– способы обеспечения информационной безопасности открытой информационной системы (З10);
– правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности открытых информационных систем (З11);

уметь:

– создавать и исследовать модели открытых систем (У1);
– разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (У2);
– проводить анализ рисков информационной безопасности автоматизированной системы (У3);
– проектировать и анализировать структуру открытых информационных систем (У4);
– применять средства защиты информационно-технологических ресурсов автоматизированной системы (У5);
– контролировать состояние подсистем информационной безопасности автоматизированной системы (У6);
– применять на практике положения нормативных документов, относящихся к обеспечению информационной безопасности открытых информационных систем (У7);
– разрабатывать политики информационной безопасности открытых информационных систем (У8);
– проектировать систему управления информационной безопасностью открытой информационной системы (У9);
– проводить анализ информационной безопасности открытой информационной системы (У10);
– формировать комплекс мер для обеспечения информационной безопасности открытых информационных систем (У11);

владеть:

– приемами и методами создания и исследования открытых систем (Н1);

– существующими моделями угроз и моделями нарушителя информационной безопасности автоматизированной системы (Н2);

– методами оценки рисков информационной безопасности автоматизированной системы (Н3);

– методологиями проектирования и анализа открытых информационных систем (Н4);

– навыками восстановления работоспособности средств защиты информации автоматизированной системы при возникновении нештатных ситуаций (Н5);

– процедурами безопасности используемыми в подсистемах информационной безопасности автоматизированной системы (Н6);

– навыками поиска нормативных документов, относящихся к обеспечению информационной безопасности открытых информационных систем (Н7);

– навыками применения положений политики информационной безопасности открытых информационных систем (Н8);

– навыками эксплуатации системы управления информационной безопасностью открытой информационной системы (Н9);

– навыками поиска и выявления проблем в системе обеспечения информационной безопасности открытой информационной системы (Н10);

– навыками применения комплекса мер для обеспечения информационной безопасности открытых информационных систем (Н11).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (практические занятия, лабораторные работы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Проектирование открытых систем.	ПК-25, ПК-26, ПСК-4.1, ПСК-4.2, ПСК-4.3, ПСК-4.4, ПСК-4.5	З5-З11, У5-У11, Н5-Н11
Тема 1.1. Стандарты открытых систем.		
Тема 1.2. Архитектура открытых систем.		
Тема 1.3. Управление инфраструктурой		
Раздел 2. Анализ безопасности.	ПК-2, ПК-4, ПК-5, ПК-8	З1-З4, У1-У4, Н1-Н4
Тема 2.1. Анализ безопасности.		
Тема 2.2. Оценка безопасности.		
Зачет	ПСК-4.1, ПСК-4.2, ПСК-4.3, ПСК-4.4, ПСК-4.5	З7-З11, У7-У11, Н7-Н11

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обучения

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Проектирование открытых систем.								
Тема 1.1. Стандарты открытых систем.	15	2	2	4		7	2	
Тема 1.2. Архитектура открытых систем.	25	4	4	8		9	2	
Тема 1.3. Управление инфраструктурой	25	4	4	8		9	2	
Раздел 2. Анализ безопасности.								
Тема 2.1. Анализ безопасности.	25	4	4	8		9	2	
Тема 2.2. Оценка безопасности.	14	2	2	4		6	2	
Зачет	4				2	2		
Итого	108 3 з.е.	16	16	32	2	42	10	0

5. Содержание разделов дисциплины

5.1. Лекции и практические занятия

Раздел 1. Проектирование открытых систем.

Тема 1.1. Стандарты открытых систем.

Лекция 1. Обзор стандартов открытых систем.

1. Особенности анализа и управления безопасностью открытых систем.
2. Классификация стандартов по безопасности
3. Серия ISO/IEC 27000. Менеджмент информационной безопасности.

Практическое занятие 1. ISO/IEC 27000.

Тема 1.2. Архитектура открытых систем.

Лекция 2. TOGAF (The Open Group Architecture Framework).

1. Введение в TOGAF.
2. Основные элементы стандарта.
3. Architecture Development Method(ADM).

Практическое занятие 2. TOGAF(The Open Group Architecture Framework).

Лекция 3. CIMOSA (Computer Integrated Manufacturing Open System Architecture).

1. Введение в CIMOSA.
2. Жизненный цикл CIM-систем.
3. Моделирование и анализ организации.

Практическое занятие 3. CIMOSA (Computer Integrated Manufacturing Open System Architecture).

Тема 1.3. Управление инфраструктурой

Лекция 4. ITIL (Information Technology Infrastructure Library).

1. Введение в ITIL.
2. ITSM (IT Service Management)
3. Рекомендации по разработке, предоставлению и управлению ИТ-сервисами.

Практическое занятие 4. ITIL (Information Technology Infrastructure Library).

Лекция 5. COBIT (Control Objectives for Information and Related Technology).

1. Введение в COBIT.
2. Факторы влияния и методология.
3. Процесс менеджмента ИТ инфраструктуры организации.

Практическое занятие 5. COBIT (Control Objectives for Information and Related Technology).

Раздел 2. Анализ безопасности

Тема 2.1. Анализ безопасности.

Лекция 6. CRAMM (CCTA Risk Analysis and Management Method).

1. Введение в CRAMM.
2. Оценка риска.
3. Выбор контрмер

Практическое занятие 6. CRAMM (CCTA Risk Analysis and Management Method).

Лекция 7. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

1. Введение в OCTAVE.
2. Профили угроз и уязвимости инфраструктуры.
3. Рекомендации по стратегии безопасности.

Практическое занятие 7. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).

Тема 2.2. Оценка безопасности.

Лекция 8. ISO/IEC 15408 Common Criteria.

1. Введение в стандарт ISO/IEC 15408.
2. Функциональные требования.
3. Требования соответствия.

Практическое занятие 8. ISO/IEC 15408 Common Criteria.

5.2. Лабораторные работы

Тема	Количество часов
Лабораторное занятие 1. ISO/IEC 27000.	2
Лабораторное занятие 2. TOGAF (The Open Group Architecture Framework).	2
Лабораторное занятие 3. CIMOSA (Computer Integrated Manufacturing Open System Architecture).	2
Лабораторное занятие 4. ITIL (Information Technology Infrastructure Library).	2
Лабораторное занятие 5. COBIT (Control Objectives for Information and Related Technology).	2
Лабораторное занятие 6. CRAMM (CCTA Risk Analysis and Management Method).	2
Лабораторное занятие 7. OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).	2
Лабораторное занятие 8. ISO/IEC 15408 Common Criteria.	2
Итого	16

5.3. Вопросы для самостоятельной работы студента в соответствии с содержанием разделов дисциплины

Раздел 1. Проектирование открытых систем.

1. История и происхождение ISO/IEC 27000.
2. История и происхождение TOGAF(The Open Group Architecture Framework).
3. История и происхождение CIMOSA (Computer Integrated Manufacturing Open System Architecture).
4. История и происхождение ITIL (Information Technology Infrastructure Library).

5. История и происхождение COBIT (Control Objectives for Information and Related Technology).

Раздел 2. Анализ безопасности.

1. История и происхождение CRAMM (CCTA Risk Analysis and Management Method).
2. История и происхождение OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
3. История и происхождение ISO/IEC 15408 Common Criteria.

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

– применения знаний на практике, поиска новой учебной информации;

– организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.).

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

– лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;

– практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.;

– лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: анализ, аннотирование и конспектирование литературы по теме, составление вопросов и тестов к теме, подготовка к лабораторным работам, подготовка реферативных сообщений.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ. Результаты самостоятельной работы учитываются при оценке знаний на зачёте.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных

целей по учебной дисциплине и проводится в форме зачета. Принимается зачет преподавателем, читающим лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся.

7.1. Вопросы к зачету

1. Что такое открытая информационная система?
2. Какими свойствами обладают открытые информационные системы?
3. На каких принципы основывается информационная безопасность открытых систем?
4. Опишите средства защиты используемые в открытых системах.
5. Опишите процессно-ориентированные стандарты и методологии (COBIT, ISM3, ISO 9001, ISO/IEC 20000, ITIL/ITSM);
6. Опишите стандарты и методологии ориентированные на лучшие практики (BSI IT-Grundschutz Catalogues, ISF Standard of Good Practice);
7. Опишите стандарты и методологии ориентированные на продукт (Common Criteria / ISO/IEC 15408);
8. Опишите стандарты и методологии ориентированные на управление рисками (AS/NZS 4360, CRAMM, EBIOS, MAGERIT, MEHARI, OCTAVE, NIST SP 800-30, SOMAP, CORAS).
9. Опишите принципы ISO/IEC 27000 Менеджмент информационной безопасности..
10. Что такое СУИБ?
11. Опишите ключевые стандарты серии ISO/IEC 27000.
12. Для чего и как используется TOGAF (The Open Group Architecture Framework)..
13. Какие элементы составляют фреймворк TOGAF?
14. Опишите метод разработки архитектуры организации в TOGAF.
15. Что такое CIMOSA (Computer Integrated Manufacturing Open System Architecture)?
16. Опишите жизненный цикл CIM-систем.
17. Как используется CIMOSA для имитационного моделирования организации?
18. Что такое ITIL (Information Technology Infrastructure Library).
19. Что такое ITSM (IT Service Management)?
20. Опишите основные рекомендации по разработке, предоставлению и управлению ИТ-сервисами в ITIL.
21. Для чего и как применяется COBIT (Control Objectives for Information and Related Technology).
22. Какие принципы лежат в основе методологии COBIT?
23. Опишите процесс менеджмента ИТ инфраструктуры организации в COBIT.
24. Для чего и как применяется CRAMM (CCTA Risk Analysis and Management Method).
25. Опишите процесс идентификации и анализа риска в CRAMM.
26. Опишите процесс выбора контрмер в CRAMM.
27. Для чего и как применяется OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation).
28. Как OCTAVE формирует профили угроз и уязвимости инфраструктуры?
29. Какие рекомендации дает OCTAVE по стратегии безопасности.
30. Какие принципы лежат в основе стандарта ISO/IEC 15408 Common Criteria?
31. Опишите классы функциональных требований ISO/IEC 15408 Common Criteria.
32. Опишите классы требований соответствия ISO/IEC 15408 Common Criteria.

7.2. Оценивание результатов зачета

Зачет проводится по окончании занятий по дисциплине до начала экзаменационной сессии в период недели контроля самостоятельной работы.

Билет для проведения промежуточной аттестации в форме зачета включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Оценка «зачтено» проставляется студенту, выполнившему и защитившему в полном объеме практические задания в течение семестра, имеются твердые и полные знания программного материала, правильные действия по применению знаний на практике, четкое изложение материала.

Оценка «не зачтено» проставляется студенту, не выполнившему и (или) не защитившему в полном объеме практические задания в течение семестра, либо наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Мельников Д.А. Информационная безопасность открытых систем. [Электронный ресурс] : учеб. – Электрон. дан. – М. : ФЛИНТА, 2014. – 448 с. – Режим доступа: http://e.lanbook.com/book/48368
2.	Тони Хаулет Защитные средства с открытыми исходными текстами. Практическое руководство по защитным приложениям [Электронный ресурс] : учебное пособие / Хаулет Тони. — Электрон. текстовые данные. — Москва, Саратов: Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 608 c. — 978-5-4487-0065-1. — Режим доступа: http://www.iprbookshop.ru/67392.html

8.2. Рекомендуемая дополнительная литература

Ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе.

№ п/п	Наименование
1.	Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. Информационные технологии для инженеров [Электронный ресурс] / С.А. Петренко, А.В. Беляев. — Электрон. текстовые данные. — Саратов: Профобразование, 2017. — 400 c. — 978-5-4488-0122-8. — Режим доступа: http://www.iprbookshop.ru/63959.html
2.	Тебайкина Н.И. Применение концепции ITSM при вводе в действие информационных систем [Электронный ресурс] : учебное пособие / Н.И. Тебайкина. — Электрон. текстовые данные. — Екатеринбург: Уральский федеральный университет, 2014. — 72 c. — 978-5-7996-1249-8. — Режим доступа: http://www.iprbookshop.ru/66578.html
3.	Скрипник Д.А. ITIL. IT Service Management по стандартам V.3.1 [Электронный ресурс] / Д.А. Скрипник. — Электрон. текстовые данные. — М. : Интернет-Университет Информационных Технологий (ИНТУИТ), 2016. — 373 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/56343.html

8.3. Правовые нормативные акты и нормативно-методические документы ограниченного доступа (доступны на кафедре)

1. Руководящий документ. Защита информации. Комплектующие помехоподавляющие изделия электронной техники, радиоэкранирующие и радиопоглощающие материалы. Общие технические требования. Утвержден приказом Гостехкомиссии России от 31.08.2001 № 355.
2. Сборник методических документов по технической защите информации ограниченного доступа, не содержащей сведений, составляющих государственную тайну, в волоконно-оптических системах передачи. Утвержден приказом ФСТЭК России от 15.03.2012 № 27.
3. Специальные требования и рекомендации по технической защите конфиденциальной информации. Утверждены приказом Гостехкомиссии России от 02.03.2001 № 282.
4. Требования к межсетевым экранам. Утверждены приказом ФСТЭК России от 09.02.2016 № 9.
5. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 06.12.2011 № 638.
6. Требования к средствам антивирусной защиты. Утверждены приказом ФСТЭК России от 20.03.2012 № 28. Требования к средствам доверенной загрузки. Утверждены приказом ФСТЭК России от 27.09.2013 № 119. Требования к средствам контроля съемных машинных носителей информации. Утверждены приказом ФСТЭК России от 28.07.2014 № 87.
7. Требованиям безопасности информации к операционным системам, утвержденным приказом ФСТЭК России от 19.08.2016 г. № 119.
8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 15.02.2008.
9. Временная методика оценки защищенности конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счет наводок на вспомогательные технические средства и системы и их коммуникации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
10. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
11. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.
12. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. Утверждена первым заместителем председателя Гостехкомиссии России 08.11.2001.

8.4. Программное обеспечение, профессиональные базы данных, информационно-справочные системы.

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.4.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)

2.	MS Windows/Linux (Ubuntu)	лицензия университета/ свободное лицензионное соглашение (http://ubuntu.ru/)
3.	SPID_AlgorithmPoC-0-4-6	https://sourceforge.net/projects/spid/files/
4.	Snort2_9_11_1	https://www.snort.org/
5.	Wireshark 2.6.3	https://www.wireshark.org/
6.	Zabbix	https://www.zabbix.com/download
7.	Clonezilla	https://clonezilla.org/downloads.php
8.	rsync	https://rsync.samba.org/
9.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
10.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218
11.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus
12.	360 Total Security	https://www.360totalsecurity.com/ru/
13.	Веб-сервер	apache https://httpd.apache.org/download.cgi
14.	Веб-препроцессор	php https://secure.php.net/downloads.php
15.	СУБД	mariadb https://mariadb.org/download/
16.	Веб-платформа	Node.js https://nodejs.org/en/download/
17.	Веб-браузер	https://www.google.com/chrome/, https://www.mozilla.org/ru/firefox/new/

8.4.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)
2.	Консультант +	
3.	База данных угроз безопасности информации	https://bdu.fstec.ru/

8.5. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	Xgu.ru.	http://xgu.ru/wiki/
2.	Российская Государственная Библиотека	http://www.rsl.ru
3.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
4.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
5.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
6.	Научная электронная библиотека	http://elibrary.ru
7.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
8.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru
9.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
10.	Информационная безопасность. Практика информационной безопасности.	http://dorlov.blogspot.com
11.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

– ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);

– мультимедийный проектор с дистанционным управлением;

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

Учебная аудитория для лабораторных занятий в области защищенных автоматизированных систем, оснащена аппаратно-программными средствами управления доступом к данным, шифрования, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, источниками бесперебойного и аварийного питания, средствами контроля и управления доступом в помещения, охранной и пожарной сигнализацией, климатическим контролем.

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться одни из следующих вариантов восприятия информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

– для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список

использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании выпускной квалификационной работы.

Формы организации студентов на лабораторных работах и практических занятиях (выбрать): фронтальная. При фронтальной форме организации занятий все студенты выполняют одновременно одну и ту же работу.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.

Лист актуализации

№ п/п	Наименование документа	Решение кафедры		Подпись	Должность, ФИО
		Дата	протокол №		