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
«АУДИТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки (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 01.12.2016 г. №1509

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Кандидат технических наук, доцент _____ А.В. Кирий

ОБСУЖДЕНО:
на заседании кафедры МиАОИС 30 «августа» 2017 г., протокол № 1

заведующий кафедрой _____ Д. В. Ильин

СОГЛАСОВАНО:

Методическая комиссия факультета ИВТ 30 «августа» 2017 г., 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

Целью дисциплины «Аудит информационных технологий и систем обеспечения информационной безопасности» является изучение методов и средств управления информационной безопасностью (ИБ) на объекте, а также на изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью определенного объекта.

Основными задачами дисциплины являются изучение основ:

- формирования требований к системе управления ИБ конкретного объекта;
- проектирование системы управления ИБ конкретного объекта;
- эффективное управление ИБ конкретного объекта.

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

Дисциплина «Аудит информационных технологий и систем обеспечения информационной безопасности» относится к обязательным дисциплинам вариативной части.

Для успешного усвоения данной дисциплины необходимо, чтобы студент владел знаниями, умениями и навыками, сформированными в процессе изучения дисциплин: «Организационное и правовое обеспечение информационной безопасности», «Открытые информационные системы», «Гуманитарные аспекты информационной безопасности».

Дисциплина является предшествующей для прохождения производственных и преддипломной практик и государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16);

способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации (ПК-17);

способность выполнять полный объем работ, связанных с реализацией частных политик информационной безопасности автоматизированной системы, осуществлять мониторинг и аудит безопасности автоматизированной системы (ПК-27);

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

Знать:

− текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ (З1);

− цели и задачи, решаемые разрабатываемыми процессами управления ИБ (З2);

− процессный подход к управлению ИБ в различных сферах деятельности (З3).

Уметь:

- определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите (У1)

- оценивать информационные риски в автоматизированных системах (У2);

− анализировать текущее состояние ИБ в организации с целью разработки требований к разрабатываемым процессам управления ИБ (У3);

− определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ (У4);

− применять процессный подход к управлению ИБ в различных сферах деятельности (У5);

− используя современные методы и средства разрабатывать процессы управления ИБ, учитывающие особенности функционирования предприятия и решаемых им задач, и оценивать их эффективность (У6);

− практически решать задачи формализации разрабатываемых процессов управления ИБ (У7);
− разрабатывать и внедрять СУИБ и оценивать ее эффективность (У8).

Владеть навыками:

- анализа информационной инфраструктуры автоматизированной системы и ее безопасности (Н1);
- методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем (Н2);
- методами оценки информационных рисков (Н3);
− терминологией и процессным подходом построения систем управления ИБ (Н4);
− навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ (Н5);
− навыками построения как отдельных процессов управления ИБ, так и системы процессов в целом (Н6).

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
Тема 1. Угрозы информационной безопасности. Инструменты аудита ИБ. Профилактика инцидентов. Тема 2. Знакомство с DLP-системами Тема 3. Контур информационной безопасности SearchInform Тема 4. Платформа SearchInform Network Sniffer Тема 5. Платформа SearchInform Endpoint Sniffer Тема 6. Управление индексами и базами данных компонентов Контура информационной безопасности SearchInform при помощи приложения SearchInform DataCenter Тема 7. Поиск по перехваченным документам при помощи приложения SearchInformClient Тема 8. Автоматический мониторинг информационных потоков при помощи приложения SearchInform AlertCenter Тема 9. Формирование отчетов об активности пользователей и инцидентах при помощи приложения SearchInform ReportCenter	ПК-16, ПК-17, ПК-27 ПСК-4.4	З1-З3 У1-У8 Н1-Н6
Зачет	ПК-16, ПК-17, ПК-27 ПСК-4.4	З1-З3, У1-У8, Н1-Н6

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			
Тема 1. Угрозы информационной безопасности. Инструменты аудита ИБ. Профилактика инцидентов.	3	1				2	1	
Тема 2. Знакомство с DLP-системами	3	1				2	1	
Тема 3. Контур информационной безопасности SearchInform	10	2	2	2		4	2	
Тема 4. Платформа SearchInform Net-workSniffer	8	2	2	2		2	2	
Тема 5. Платформа SearchInform End-pointSniffer	8	2	2	2		2	2	
Тема 6. Управление индексами и базами данных компонентов Контура информационной безопасности SearchInform при помощи приложения SearchInform DataCenter	12	2	4	2		4	2	
Тема7. Поиск по перехваченным документам при помощи приложения SearchInform Client	8	2	2	2		2	2	
Тема 8. Автоматический мониторинг информационных потоков при помощи приложения SearchInform AlertCenter	8	2	2	2		2	2	
Тема 9. Формирование отчетов об активности пользователей и инцидентах при помощи приложения SearchInformReportCenter	10	2	2	4	2	2	2	
Зачет	2				2			
Итого	72 2 з.е.	16	16	16	2	22	16	0

5. Содержание разделов дисциплины

5.1. Лекции

Тема 1. Угрозы информационной безопасности. Инструменты аудита ИБ. Профилактика инцидентов.
Тема 2. Знакомство с DLP-системами
Тема 3. Контур информационной безопасности SearchInform
Тема 4. Платформа SearchInform Network Sniffer
Тема 5. Платформа SearchInform Endpoint Sniffer
Тема 6. Управление индексами и базами данных компонентов Контура информационной безопасности SearchInform при помощи приложения SearchInform DataCenter
Тема 7. Поиск по перехваченным документам при помощи приложения SearchInform Client
Тема 8. Автоматический мониторинг информационных потоков при помощи приложения SearchInform AlertCenter
Тема 9. Формирование отчетов об активности пользователей и инцидентах при помощи приложения SearchInform ReportCenter

5.2. Лабораторные работы и практические занятия

Тема	Количество часов л/р	Количество часов п/р
1. Платформа SearchInformNetworkSniffer	4	2
2. Платформа SearchInformEndpointSniffer	2	2
3. Управление индексами и базами данных компонентов Контура информационной безопасности SearchInform при помощи приложения SearchInformDataCenter	2	4
4. Поиск по перехваченным документам при помощи приложения SearchInformClient	4	2
5. Автоматический мониторинг информационных потоков при помощи приложения SearchInformAlertCenter	2	2
6. Формирование отчетов об активности пользователей и инцидентах при помощи приложения SearchInformReportCenter	2	4
Итого	16	16

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).

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: подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание устного выступления студента на практическом занятии, его доклада; проверка письменных отчётов по результатам выполненных заданий и лабораторных работ; защита исследовательской работы. 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 и задания к зачету

1. Для защиты от каких типовых угроз применяются DLP-системы?
2. Охарактеризуйте типы и категории нарушителей, для борьбы с которыми могут быть использованы DLP-системы.
3. Что понимается под DLP?
4. Опишите принципы функционирования DLP-системы.
5. Охарактеризуйте основные этапы развития DLP-систем.
6. Охарактеризуйте назначение систем идентификации и аутентификации.
7. Охарактеризуйте назначение SIEM-систем.
8. Охарактеризуйте назначение сетевых анализаторов трафика/снифферов.
9. Перечислите плюсы и минусы различных способов перехвата информации в компьютерных сетях.
10. Для чего предназначена DLP-система «Контур информационной безопасности SearchInform» (далее – КИБ)?
11. Охарактеризуйте архитектуру DLP-системы КИБ. Какие компоненты относятся к серверной части, а какие – к клиентской?
12. Какие виды перехвата данных реализованы при помощи платформы NetworkSniffer?
13. Какие виды перехвата данных реализованы при помощи платформы EndpointSniffer?
14. Опишите общую схему движения информации в КИБ.
15. Какие СУБД могут быть использованы совместно с КИБ?
16. Какие компоненты платформ КИБ помещают перехваченные сообщения и файлы в базы данных, а какие – в хранилища?
17. Какую роль в функционировании КИБ играет сервер SoftInform Search?
18. Какой продукт используется в КИБ для управления индексами и базами данных? Охарактеризуйте его основные функции.
19. Перечислите основные виды поиска, используемые компонентом SearchInformClient.
20. Перечислите основные задачи, решаемые при помощи компонента SearchInform AlertCenter.
21. Укажите назначение и основные функции компонента SearchInform ReportCenter.
22. Перечислите и охарактеризуйте ключевые функции платформы SearchInform NetworkSniffer.
23. Под управлением каких операционных систем семейства Windows может работать Searchinform NetworkSniffer?

24. Под управлением каких СУБД должен функционировать сервер баз данных перехваченных документов?
25. Назовите основные способы интеграции SearchInform NetworkSniffer в сетевую структуру.
26. Каковы особенности перенаправления трафика при помощи устройств с функцией зеркалирования?
27. Каковы особенности реализации перенаправления трафика между прокси-сервером и интернетом?
28. Каковы особенности реализации перенаправления трафика при использовании терминальных серверов?
29. Какие права должны быть настроены для доменных пользователей, под учетными записями которых будут работать сервисы, входящие в состав SearchInformNetworkSniffer?
30. Опишите основные настройки входа службы перехвата.
31. Охарактеризуйте используемые уровни логирования.
32. Какие опции должны быть отключены в настройках сетевых карт для предотвращения потери пакетов?
33. Перечислите и охарактеризуйте ключевые функции платформы SearchInform Endpoint Sniffer.
34. Под управлением каких операционных систем семейства Windows может работать SearchInform Endpoint Sniffer?
35. Под управлением каких СУБД должен функционировать сервер баз данных перехваченных документов?
36. Опишите принцип работы SearchInform Endpoint Sniffer.
37. Перечислите способы, с помощью которых агент может быть установлен на рабочую станцию.
38. Опишите особенности процедуры установки агентов средствами групповых политик.
39. Какие задачи можно решить при помощи индивидуальной настройки агентов*?*
40. В каких случаях может применяться режим блокировки исходящей почты?
41. Для чего может понадобиться настройка учетной записи, под которой будет функционировать установленный агент?
42. Каким образом осуществляется настройка расписания передачи данных агентами на сервер?
43. Каковы признаки того, что первая установка агента на рабочую станцию прошла успешно?
44. Опишите порядок работы агента применительно к перехвату информации.
45. Как можно осуществлять «балансировку» загруженности канала при передаче данных от агента на сервер?
46. Для чего нужны «ограничительные» опции «максимальный размер очереди» и «минимальное свободное место на диске» в настройках агента?
47. Для чего нужны «Альтернативные адреса ES»?
48. Какие настройки необходимо выполнить, чтобы полностью заблокировать возможность передачи данных с компьютера на мобильный телефон?
49. Для чего предназначен агент Device Sniffer?
50. Перечислите ограничения на передачу данных, которые можно задавать в агенте DeviceSniffer?
51. Какова роль «Белого списка» в агенте Device Sniffer?
52. Каким образом осуществляется настройка доступа и аудита внешнего устройства для отдельного пользователя?
53. Какие ограничения в агенте Device Sniffer имеют приоритет: по пользователю или по компьютеру?

54. Для чего предназначен агент File Sniffer?
55. Каковы особенности применения правил аудита к пользователям?
56. Каковы особенности применения правил аудита к файлам и процессам?
57. Для чего предназначен агент Mail Sniffer?
58. Для чего предназначен агент Microphone Sniffer?
59. Как в агенте Microphone Sniffer определяется, какой из наборов настроек «В офисе»/«Вне офиса» следует применять в данный момент времени?
60. Для чего предназначен агент Monitor Sniffer?
61. В каких режимах может работать перехват агента Monitor Sniffer?
62. Для чего в Monitor Sniffer реализован перехват фактов посещения определённых URL?
63. Как можно минимизировать размеры сохраняемых изображений экрана в агенте MonitorSniffer?
64. Для чего предназначен агент Print Sniffer?
65. С какой целью используется опция «Блокировка Escape функций»?
66. Для чего предназначен агент Skype Sniffer?
67. Для чего предназначен агент Mobile Sniffer?
68. Каким образом осуществляется просмотр текущей активности сервера ES?
69. Через какой порт осуществляется взаимодействие серверов EndpointSniffer и SoftInformSearch?
70. Какова роль фильтрации в платформе SearchInform Endpoin Sniffer?
71. По каким основаниям может осуществляться фильтрация в платформе SearchInform Endpoin Sniffer?
72. Как осуществляется перехват трафика, передаваемого по защищенному SSL-соединению?
73. Перечислите и охарактеризуйте ключевые функции SearchInform Data Center.
74. Какие операции позволяет осуществлять консоль SearchInform Data Center?
75. Какими способами можно осуществлять запуск сервера Data Center?
76. Как осуществляется задание БД по умолчанию?
77. Как осуществляется настройка сервера Data Center?
78. Зачем необходимо осуществлять настройку синхронизации с Active Directory?
79. Для каких событий можно настроить уведомления?
80. Какие цели преследует автоматическое управление компонентами КИБ?
81. Для чего необходимо «разбивать» индексы?
82. Опишите разграничение прав, реализованное в модуле DataCenter.
83. Назовите назначение и область применения программного продукта SearchInformClient.
84. Перечислите и охарактеризуйте ключевые функции SearchInformClient.
85. Для чего может быть использована консоль SearchInformClient?
86. Охарактеризуйте основные элементы интерфейса консоли SearchInformClient.
87. Опишите особенности подключения к индексам сервера индексации.
88. Какие опции могут быть использованы для настройки текстового поиска?
89. Опишите особенности использования поиска по словарю.
90. Охарактеризуйте особенности использования алгоритма «поиск похожих».
91. Назовите параметры, используемые в SearchInformClient, для ограничения результатов поиска.
92. Что необходимо сделать для ограничения результатов поиска по дате, времени и размеру перехваченных файлов?
93. Что необходимо сделать для ограничения результатов поиска по домену и доменным пользователям?
94. Что необходимо сделать для исключения из результатов поиска документов, при передаче которых использовалось безопасное соединение (протокол SSL)?

95. Что необходимо сделать для ограничения результатов поиска по именам компьютеров, IP-/MAC-адресам, именам и типам файлов?
96. Что необходимо сделать для ограничения результатов поиска по атрибутам документа?
97. Опишите основные правила использования модификаторов.
98. Охарактеризуйте режимы просмотра информации на панели результатов.
99. На что указывает цвет, которым в результатах выдачи могут маркироваться документы?
100. С какой целью может быть использована группировка по заголовкам столбцов на панели результатов?
101. Охарактеризуйте режимы отображения информации в окне предпросмотра.
102. Опишите правила настройки псевдонимов для эффективного поиска по индексу IMSniffer.
103. Назовите назначение и область применения программного продукта SearchInformAlertCenter.
104. Перечислите и охарактеризуйте ключевые функции SearchInform AlertCenter.
105. Из каких частей состоит SearchInform AlertCenter?
106. Опишите функции и интерфейс серверного модуля SearchInform AlertCenter.
107. Опишите функции и интерфейс клиентского модуля SearchInform AlertCenter.
108. Каким образом осуществляется подключение индексов и баз данных для работы SearchInform AlertCenter?
109. Каким образом осуществляется регистрация пользователей SearchInform AlertCenter?
110. Как осуществляется настройка политик безопасности? Приведите пример.
111. Опишите особенности применения фразового поиска для нахождения содержащих критичную информацию документов.
112. Опишите особенности применения поиска по словарю.
113. С какой целью может быть использован алгоритм «поиск похожих»?
114. Опишите особенности применения поиска по атрибутам.
115. Для решения каких задач может быть использован поиск нераспознанных документов?
116. Как формируются запросы с использованием регулярных выражений?
117. Как формируются запросы с использованием цифровых отпечатков?
118. Опишите особенности формирования сложных запросов?
119. Как осуществляется настройка индексов для анализа в процессе создания политики безопасности?
120. Как осуществляется настройка списка получателей уведомлений в процессе создания политики безопасности?
121. Как осуществляется настройка списка исключений в процессе создания политики безопасности?
122. Как осуществляется настройка расписания проверок в процессе создания политики безопасности?
123. Как осуществляется управление журналом инцидентов?
124. Какие возможности пользователю SearchInformAlertCenter предоставляет фильтрация списка инцидентов?
125. Как и с какой целью осуществляется настройка политик карантина?
126. Опишите общие настройки SearchInformAlertCenter.
127. Каким образом осуществляется настройка отправки уведомлений (узел настроек «Параметры»)?
128. Каким образом осуществляется настройка списков исключений (узел настроек «Параметры»)?
129. По каким параметрам пользователь может быть исключен из проверки?

130. Опишите процедуры формирования и управления словарями синонимов.
131. Опишите процедуры настройки библиотеки регулярных выражений.
132. Опишите процедуры настройки библиотеки цифровых отпечатков.
133. Опишите основные правила использования журналов событий.
134. Назовите назначение и область применения программного продукта SearchInform Report Center.
135. Из каких частей состоит SearchInform Report Center?
136. Опишите функции и интерфейс клиентской части Report Center.
137. Каким образом осуществляется подключение к базе Report Center?
138. Как осуществляется выбор временного периода, за который будет сгенерирован тот или иной отчет?
139. Как осуществляется выбор пользователей, по которым будет сгенерирован тот или иной отчет?
140. Охарактеризуйте общие шаблоны отчетов, которые включены в базовую поставку Report Center.
141. Охарактеризуйте шаблоны отчетов по продуктам, которые включены в базовую поставку Report Center.
142. Какие формы используются для представления отчетов?
143. Перечислите, какие операции могут производиться в окне просмотра отчетов?
144. Охарактеризуйте возможности детализации отчетов.
145. Охарактеризуйте возможности навигации по отчетам.
146. Опишите процедуру создания нового шаблона отчета.
147. Опишите особенности редактирования пользовательского шаблона.
148. Каким образом можно выбрать, какие шаблоны будут отображаться в главном окне клиента, а какие – нет?
149. Каким образом и с какой целью может осуществляться вызов внешнего приложения (например, приложения SearchInform Client)?
150. Охарактеризуйте область применения отчетов в виде графа отношений.
151. Каким образом с помощью графа отношений можно решить задачу получения данных о контактах внешнего пользователя с внутренними (сотрудниками компании)?
152. Для чего предназначены отчеты Endpoint Sniffer?
153. Какими командами необходимо воспользоваться для просмотра перечня установленного на компьютерах программного обеспечения?
154. Какими командами необходимо воспользоваться для просмотра истории установки и удаления на компьютерах программного обеспечения?
155. Какими командами необходимо воспользоваться для просмотра истории установки агентов?
156. Какими командами необходимо воспользоваться для просмотра количества сообщений, отправленных компьютерами, по каждому продукту?

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.	Анализ состояния защиты данных в информационных системах [Электронный ресурс] : учебно-методическое пособие / В.В. Денисов. — Электрон. текстовые данные. — Новосибирск: Новосибирский государственный технический университет, 2012. — 52 c. — 978-5-7782-1969-4. — Режим доступа: http://www.iprbookshop.ru/44897.html
2.	Демидов А.А. Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления [Электронный ресурс] : учебное пособие / А.А. Демидов. — Электрон. текстовые данные. — СПб. : Университет ИТМО, 2015. — 70 c. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/67555.html
3.	Паршин К.А. Оценка уровня информационной безопасности на объекте информатизации [Электронный ресурс] : учебное пособие / К.А. Паршин. — Электрон. текстовые данные. — М. : Учебно-методический центр по образованию на железнодорожном транспорте, 2015. — 96 c. — 978-5-89035-821-9. — Режим доступа: http://www.iprbookshop.ru/45291.html

8.2. Рекомендуемая дополнительная литература

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

№ п/п	Наименование
1.	Аккредитация и аттестация [Электронный ресурс] : сборник нормативных актов и документов / . — Электрон. текстовые данные. — Саратов: Ай Пи Эр Медиа, 2015. — 77 c. — 978-5-905916-68-7. — Режим доступа: http://www.iprbookshop.ru/30281.html
2.	Герасимов, А.А. Обследование объектов информатизации: методические указания к выполнению лабораторной работы по курсу «Аттестация объектов информатизации» [Электронный ресурс] : метод. указ. / А.А. Герасимов, Е.В. Вайц. — Электрон. дан. — Москва : МГТУ им. Н.Э. Баумана, 2012. — 28 с. — Режим доступа: https://e.lanbook.com/book/62002. — Загл. с экрана.
3.	Дураковский А.П., Куницын И.В., Лаврухин Ю.Н. Контроль защищенности речевой информации в помещениях. Аттестационные испытания вспомогательных технических средств и систем по требованиям безопасности информации.: Учебное пособие. – М.: НИЯУ МИФИ, 2015. – 152 с.

Нормативные правовые и методические документы в области защиты информации доступны по ссылке https://fstec.ru/component/tags/tag/informatsionnoe-soobshchenie

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.	Система обнаружения вторжений	Snort https://www.snort.org/
14.	Средства дублирования и восстановления данных	Clonezilla https://clonezilla.org/downloads.php, rsync https://rsync.samba.org/
15.	Средства мониторинга состояния автоматизированных систем	Zabbix https://www.zabbix.com/download

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».

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. 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: групповая. При групповой форме организации занятий одна и та же работа выполняется бригадами по 2 - 5 человек.

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.