САМАРСКИЙ ПОЛИТЕХ
Самарский университет

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Директор филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
_____ / Г.И. Заболотни
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ФТД.В.01 «Основы информационной безопасности»

Код и направление подготовки (специальность)	13.03.02 Электроэнергетика и электротехника
Направленность (профиль)	Электроэнергетика
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2024
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Кафедра-разработчик	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Объем дисциплины, ч. / з.е.	36 / 1
Форма контроля (промежуточная аттестация)	Зачет

Самара 2024

ФТД.В.01 «Основы информационной безопасности»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **13.03.02 Электроэнергетика и электротехника**, утвержденного приказом Министерства образования и науки РФ от № 144 от 28.02.2018 и соответствующего учебного плана.

Разработчик РПД:

(должность, степень, ученое звание)	(ФИО)

Заведующий кафедрой	А.А. Складчиков, кандидат технических наук
	(ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	
	(ФИО, степень, ученое звание)
Руководитель образовательной программы	
	(ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Универсальные компетенции			
Безопасность жизнедеятельности	УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций и военных конфликтов	Владеть навыками использования методов организации и контроля функционирования системы защиты информации навыками использования стандартов для защиты информации в информационной системе
			Знать основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации содержание основных уровней обеспечения информационной безопасности
			Уметь выполнять анализ требований к системе защиты информации выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **блок факультативных дисциплин**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины
УК-8		Безопасность жизнедеятельности; Основы военной подготовки	Государственная итоговая аттестация: подготовка к процедуре защиты и защита выпускной квалификационной работы; Экология

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	4 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	16	16
Лекции	4	4
Практические занятия	12	12
Самостоятельная работа (всего), в том числе:	20	20
выполнение задач, заданий, упражнений (в том числе разноуровневых)	10	10
подготовка к зачету	10	10
Итого: час	36	36
Итого: з.е.	1	1

4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Основы информационной безопасности	4	0	12	20	36
	Итого	4	0	12	20	36

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
4 семестр				
1	Основы информационной безопасности	Изучение методов оценивания воздействия ИКТ-технологий на неприкосновенность частной жизни.	Воспитание ответственного отношения к информационной деятельности, связанной с обработкой и хранением информации; Приобретение опыта профилактической и предупреждающей деятельности по отношению к информационным угрозам на уровне личной информационной безопасности	2
2	Основы информационной безопасности	Изучение методики управления рисками для анализа рисков личной информационной безопасности	Изучить методику для систематизации и анализа рисков по приведенным в приложении материалам курса С.А.Нестерова и "Руководства по управлению рисками". На основании собранных на лабораторном занятии №1 данных о неприкосновенность частной жизни идентифицировать риски личной информационной безопасности и создать их полное описание по определению методики. Выполнить этап "Поддержка принятия решений". Разработать план мероприятий по осуществлению этапов "Реализация контроля" и "Оценка эффективности программы".	2
			Итого за семестр:	**4**
			Итого:	**4**

4.2 Содержание лабораторных занятий

Учебные занятия не реализуются.

4.3 Содержание практических занятий

№ занятия	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
4 семестр				
1	Основы информационной безопасности	Аутентификация, разрешениями на файлы и папки Управление	Управления разрешениями на файлы и папки Windows. Управление доступом к файлам.	2
2	Основы информационной безопасности	Настройка Интернет-браузера для безопасной работы	Изучение настроек безопасности для различных браузеров.	2

3	Основы информационной безопасности	Разработка политики информационной безопасности	Разработать политику информационной безопасности подразделения с использованием общепринятых шаблонов и учетом специфики деятельности организации.	2
4	Основы информационной безопасности	Обзор функций безопасности Windows	Приобрести практические навыки использования технологий BitLocker, IPSec, MMC, UAC, встроенных в Windows.	2
5	Основы информационной безопасности	Анализ безопасности протокола обмена информацией	Найти уязвимость в схеме протокола. Определить, атака какого типа позволит воспользоваться выявленной уязвимостью протокола. Предложить способ модифицировать протокол, чтобы устранить уязвимость.	2
6	Основы информационной безопасности	Применение методики управления рисками для анализа рисков личной информационной безопасности	Изучить методику для систематизации и анализа рисков по приведенным в приложении материалам курса С.А.Нестерова и "Руководства по управлению рисками". На основании собранных на лабораторном занятии №1 данных о неприкосновенность частной жизни идентифицировать риски личной информационной безопасности и создать их полное описание по определению методики. Выполнить этап "Поддержка принятия решений". Разработать план мероприятий по осуществлению этапов "Реализация контроля" и "Оценка эффективности программы".	2
			Итого за семестр:	**12**
			Итого:	**12**

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
4 семестр			
Основы информационной безопасности	Подготовка к зачёту	Повторение всех тем входящих в дисциплину.	20
		Итого за семестр:	**20**
		Итого:	**20**

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	**Библиографическое описание**	**Ресурс НТБ СамГТУ** (ЭБС СамГТУ, IPRbooks и т.д.)

1	Технологии и продукты Microsoft в обеспечении информационной безопасности; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||102070	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	Microsoft Windows	Windows (Зарубежный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Практические занятия

401 (учебный корпус)

Компьютерный класс – учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации – лингафонный кабинет.

Технические средства обучения, служащие для представления учебной информации большой аудитории, набор демонстрационного оборудования: экран, проектор, переносной ноутбук.

Оборудование: 18 компьютеров с выходом в сеть Интернет и с доступом в электронную информационно-образовательную среду СамГТУ.

Специализированная мебель: 18 компьютерных столов, 18 кресел-комфорт, стол и стул для преподавателя, доска.

Лабораторные занятия

209 (учебный корпус)

Помещение для самостоятельной работы – учебная аудитория для курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций.

Аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет» и с доступом в электронную информационно- образовательную среду СамГТУ.

Оборудование: 10 компьютеров с выходом в сеть Интернет.

Специализированная мебель:10 компьютерных стола, 10 стульев.

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим

занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
ФТД.В.01 «Основы информационной безопасности»

Фонд оценочных средств
по дисциплине
ФТД.В.01 «Основы информационной безопасности»

Код и направление подготовки (специальность)	13.03.02 Электроэнергетика и электротехника
Направленность (профиль)	Электроэнергетика
Квалификация	Бакалавр
Форма обучения	Очная
Год начала подготовки	2024
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Кафедра-разработчик	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Объем дисциплины, ч. / з.е.	36 / 1
Форма контроля (промежуточная аттестация)	Зачет

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Универсальные компетенции			
Безопасность жизнедеятельности	УК-8 Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов	УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций и военных конфликтов	Владеть навыками использования методов организации и контроля функционирования системы защиты информации навыками использования стандартов для защиты информации в информационной системе
			Знать основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации содержание основных уровней обеспечения информационной безопасности
			Уметь выполнять анализ требований к системе защиты информации выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе

Матрица соответствия оценочных средств запланированным результатам обучения

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Основы информационной безопасности				
УК-8.2 Понимает, как создавать и поддерживать безопасные условия жизнедеятельности, том числе при возникновении чрезвычайных ситуаций и военных конфликтов	**Уметь** выполнять анализ требований к системе защиты информации выявлять угрозы информационной безопасности, обосновывать организационно-технические мероприятия по защите информации в информационной системе	вопросы	Да	Да
	Знать основные законодательные и нормативные документы федерального уровня в области информационной безопасности и защиты информации содержание основных уровней обеспечения информационной безопасности	вопросы	Да	Да
	Владеть навыками использования методов организации и контроля функционирования системы защиты информации навыками использования стандартов для защиты информации в информационной системе	вопросы	Да	Да

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Формы текущей/промежуточной аттестации

Текущая аттестация студентов производится на практических и лабораторных занятиях в форме устного опроса и проверка отчетов по лабораторным работам. Промежуточная аттестация студентов проводится в форме зачета с оценкой. Для подготовки к промежуточной аттестации студентам выдается список вопросов для проведения зачета.

Перечень вопросов для промежуточной аттестации (Экзамен)

1) Определение, свойства, виды и формы представления информации;
2) Аттестация объектов по требованиям безопасности;
3) Анализ информационных ресурсов на предприятии;
4) Организация и планирование безопасности компьютерных систем;
5) Факторы и критерии принятия решения о защите компьютерных систем;
6) Лицензирование и сертификация средств защиты информации;
7) Понятие информационной безопасности;
8) Объекты информационной безопасности Российской Федерации;
9) Государственные стандарты в области защиты информации;
10) Экономические аспекты обеспечения безопасности сложных систем;
11) Правовые и организационно-технические вопросы безопасности компьютерных систем;
12) Понятие и виды конфиденциальной информации;
13) Защита конфиденциальной информации;
14) Угрозы информационной безопасности и их классификация;
15) Структура и основные элементы модели нарушителя;
16) Объекты, цели и задачи защиты компьютерных систем;
17) Категорирование ресурсов компьютерных систем и определение требований к уровню обеспечения их безопасности;
18) Принципы защиты компьютерных систем;
19) Аудит информационной безопасности, алгоритмы и методы аудита информационной безопасности;
20) Комплексный анализ безопасности компьютерных систем на методологическом, организационно-управленческом, технологическом и техническом уровнях;
21) Стратегия управления информационными рисками на основе получения их качественных и количественных оценок;
22) Понятие и признаки компьютерных преступлений, классификация компьютерных преступлений;
23) Компьютерные вирусы и принципы их функционирования;
24) Программные антивирусные средства;
25) Проблемы обеспечения программно-технологической безопасности компьютерных систем;
26) Технологическая безопасность и жизненный цикл компьютерных систем;

27) Требования, предъявляемые к архитектуре баз данных для обеспечения безопасности функционирования компьютерных систем;
28) Средства собственной защиты информационных систем;
29) Средства активной защиты компьютерных систем;
30) Средства пассивной защиты компьютерных систем;
31) Защита памяти компьютерных систем;
32) Защита выполнения программ компьютерных систем;
33) Защиты дисков компьютерных систем;
34) Средства защиты программного обеспечения с электронными ключами;
35) Уровни инфраструктуры информационной сети, источники уязвимости информационной сети;
36) Классификация атак и типовой сценарий действий потенциальных нарушителей инфраструктуры информационной сети;
37) Защитные механизмы и средства обеспечения безопасности информационной сети;
38) Краткая характеристика протоколов сетевого взаимодействия;
39) Проблемы обеспечения безопасности сетевых ОС;
40) Критерии оценки защищенности ОС;
41) Мероприятия по настройке системы безопасности сетевых ОС;
42) Криптография и криптология;
43) Обобщенная схема криптосистемы;
44) Теоретическая, практическая и временная стойкость системы криптографической защиты;
45) Симметричные алгоритмы шифрования;
46) Алгоритм шифрования DES;
47) Методы генерации псевдослучайных чисел;
48) Асимметричные алгоритмы шифрования;
49) Стандарт шифрования RSA;
50) Электронная цифровая подпись;
51) Криптографические протоколы;
52) Информационная безопасность баз данных;
53) Защита информационных ресурсов в сетях, подключенных к Internet;
54) Технические каналы утечки информации.

Дополнительная литература

1) Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
2) Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных».
3) ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения.
4) Савельев А.И. Лицензирование программного обеспечения в России: Законодательство и практика. – Infotropic Media, 2012. – 432 с.
5) Борисов, А. Н. Комментарий к Федеральному закону от 4 мая 2011 г. №99-ФЗ "О лицензировании отдельных видов деятельности" (постатейный) / А.Н. Борисов. - М.: Юстицинформ, 2016. - 226 с.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

Формы текущей/промежуточной аттестации

Текущая аттестация студентов производится на практических и лабораторных занятиях в форме устного опроса и проверка отчетов по лабораторным работам. Промежуточная аттестация студентов проводится в форме зачета с оценкой. Для подготовки к промежуточной аттестации студентам выдается список вопросов для проведения зачета.

Перечень вопросов для промежуточной аттестации (Экзамен)

1) Определение, свойства, виды и формы представления информации;
2) Аттестация объектов по требованиям безопасности;
3) Анализ информационных ресурсов на предприятии;
4) Организация и планирование безопасности компьютерных систем;
5) Факторы и критерии принятия решения о защите компьютерных систем;
6) Лицензирование и сертификация средств защиты информации;
7) Понятие информационной безопасности;
8) Объекты информационной безопасности Российской Федерации;
9) Государственные стандарты в области защиты информации;
10) Экономические аспекты обеспечения безопасности сложных систем;
11) Правовые и организационно-технические вопросы безопасности компьютерных систем;
12) Понятие и виды конфиденциальной информации;
13) Защита конфиденциальной информации;
14) Угрозы информационной безопасности и их классификация;
15) Структура и основные элементы модели нарушителя;
16) Объекты, цели и задачи защиты компьютерных систем;
17) Категорирование ресурсов компьютерных систем и определение требований к уровню обеспечения их безопасности;
18) Принципы защиты компьютерных систем;
19) Аудит информационной безопасности, алгоритмы и методы аудита информационной безопасности;
20) Комплексный анализ безопасности компьютерных систем на методологическом, организационно-управленческом, технологическом и техническом уровнях;
21) Стратегия управления информационными рисками на основе получения их качественных и количественных оценок;
22) Понятие и признаки компьютерных преступлений, классификация компьютерных преступлений;
23) Компьютерные вирусы и принципы их функционирования;
24) Программные антивирусные средства;
25) Проблемы обеспечения программно-технологической безопасности компьютерных систем;
26) Технологическая безопасность и жизненный цикл компьютерных систем;

27) Требования, предъявляемые к архитектуре баз данных для обеспечения безопасности функционирования компьютерных систем;
28) Средства собственной защиты информационных систем;
29) Средства активной защиты компьютерных систем;
30) Средства пассивной защиты компьютерных систем;
31) Защита памяти компьютерных систем;
32) Защита выполнения программ компьютерных систем;
33) Защиты дисков компьютерных систем;
34) Средства защиты программного обеспечения с электронными ключами;
35) Уровни инфраструктуры информационной сети, источники уязвимости информационной сети;
36) Классификация атак и типовой сценарий действий потенциальных нарушителей инфраструктуры информационной сети;
37) Защитные механизмы и средства обеспечения безопасности информационной сети;
38) Краткая характеристика протоколов сетевого взаимодействия;
39) Проблемы обеспечения безопасности сетевых ОС;
40) Критерии оценки защищенности ОС;
41) Мероприятия по настройке системы безопасности сетевых ОС;
42) Криптография и криптология;
43) Обобщенная схема криптосистемы;
44) Теоретическая, практическая и временная стойкость системы криптографической защиты;
45) Симметричные алгоритмы шифрования;
46) Алгоритм шифрования DES;
47) Методы генерации псевдослучайных чисел;
48) Асимметричные алгоритмы шифрования;
49) Стандарт шифрования RSA;
50) Электронная цифровая подпись;
51) Криптографические протоколы;
52) Информационная безопасность баз данных;
53) Защита информационных ресурсов в сетях, подключенных к Internet;
54) Технические каналы утечки информации.

Дополнительная литература

1) Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ (последняя редакция).
2) Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) «О правовой охране программ для электронных вычислительных машин и баз данных».
3) ГОСТ Р 54593-2011 Информационные технологии (ИТ). Свободное программное обеспечение. Общие положения.
4) Савельев А.И. Лицензирование программного обеспечения в России: Законодательство и практика. – Infotropic Media, 2012. – 432 с.
5) Борисов, А. Н. Комментарий к Федеральному закону от 4 мая 2011 г. №99-ФЗ "О лицензировании отдельных видов деятельности" (постатейный) / А.Н. Борисов. - М.: Юстицинформ, 2016. - 226 с.