МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

КОМПЛЕКСНЫЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ

Направление подготовки 10.03.01 Информационная безопасность

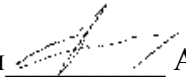
Направленность «Организация и технология защиты информации»

Квалификация (степень) выпускника: Бакалавр

Кострома

Рабочая программа дисциплины «Комплексные системы защиты информации на предприятии» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования направления подготовки 10.03.01 Информационная безопасность, утвержден 01.12.2016 г.

Год начала подготовки 2017

Разработал  Алексеев Дмитрий Станиславович, доцент кафедры защиты информации, к.т.н.

Рецензент:  _Щекочихин Олег Владимирович, к.т.н., доцент, заведующий кафедры защиты информации

УТВЕРЖДЕНО:

На заседании кафедры защиты информации

Протокол заседания кафедры № 13 от 6 июля 2017 г.

Заведующий кафедрой защиты информации

 _____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № 12 от 27 июня 2018 г.

Заведующий кафедрой защиты информации

 _____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _11_ от _30.05.2019_____ г.

Заведующий кафедрой защиты информации

 _____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _8_ от _6.04.2020_____ г.

Заведующий кафедрой защиты информации


_____Щекочихин Олег Владимирович, к.т.н., доцент

ПРОГРАММА ПЕРЕУТВЕРЖДЕНА:

На заседании кафедры защиты информации:

Протокол заседания кафедры № _6_ от _22.01.2021_____ г.

Заведующий кафедрой защиты информации


_____Щекочихин Олег Владимирович, к.т.н., доцент

1. Цели и задачи освоения дисциплины

Целями дисциплины «Комплексные системы защиты информации на предприятии» являются обеспечение подготовки бакалавров в соответствии с требованиями ФГОС ВО и учебного плана по направлению 10.03.01 «Информационная безопасность»; формирование компетентности в области разработки комплексной системы защиты информации предприятия, на основе оценки угроз безопасности информации, способов моделирования, технологии организации, кадрового, технологического и нормативно-методического обеспечения, методах оценки эффективности подобных систем.

Предмет курса:

- система защиты информации;
- анализ и оценки угроз защищаемой информации;
- модель процессов защиты информации;
- технологическое и организационное построение системы защиты информации;
- кадровое, материально-техническое и нормативно-методическое обеспечение защиты информации на предприятии;
- планирование и контроль комплексной системы защиты информации на предприятии;
- эффективность системы защиты информации;
- аттестации объектов информатизации по требованиям безопасности информации.

Профессиональные цели курса - формирование знаний в области концептуальных основ разработки комплексной системы защиты информации и определения объектов защиты.

Задачи дисциплины:

- изучение сущности, целей и задач комплексной системы защиты информации;
- изучение принципов и этапов разработки комплексной системы защиты информации;
- освоение технологии установления состава защищаемой информации и объектов защиты информации на предприятии;
- овладение методами оценки угроз безопасности информации;
- изучение параметров и структуры комплексной системы защиты информации;
- установление состава мероприятий по обеспечению функционирования комплексной системы защиты информации;
- изучение показателей и методик эффективности системы защиты информации.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

знать

- понятие, сущность, цели и задачи комплексной системы защиты информации;
- принципы организации и этапы разработки комплексной системы защиты информации;
- факторы, влияющие на организацию комплексной системы защиты информации;
- технологию определения состава защищаемой информации и объектов защиты;
- методы моделирования, анализа и оценки угроз защищаемой информации;
- виды моделей, описывающих процессы защиты информации;
- содержание технологического и организационного построения системы защиты информации на предприятии;
- состав мероприятий и условия, обеспечивающие функционирование системы защиты информации на предприятии;
- порядок кадрового, материально-технического и нормативно-методического обеспечения защиты информации на предприятии;
- порядок организации планирования и контроля комплексной системы защиты информации на предприятии;

- методику анализа эффективности системы защиты информации;
- порядок организации аттестации объектов информатизации по требованиям безопасности информации;

уметь

- классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности;
- классифицировать и оценивать угрозы информационной безопасности для объекта информатизации;
- формировать комплекс мер по защите информации на предприятии и оценивать их эффективность на основе заданных требований по безопасности информации;
- разрабатывать проекты нормативных и организационно-распорядительных документов, регламентирующих работу по защите информации на предприятии;

владеть

- методиками проверки защищенности объектов информатизации на соответствие требованиям безопасности информации;
- технологией разработки организационно-функциональной структуры и комплекса нормативно-методического обеспечения комплексной защиты информации на предприятии.

освоить компетенции:

- способность выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);
- способность администрировать подсистемы информационной безопасности объекта защиты (ПК-3);
- способность участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);
- способность проводить совместный анализ функционального процесса объекта защиты и его информационных составляющих с целью определения возможных источников информационных угроз, их вероятных целей и тактики (ПСК-2.1);
- способность формировать предложения по оптимизации функционального процесса объекта защиты и его информационных составляющих с целью повышения их устойчивости к деструктивным воздействиям на информационные ресурсы и предложения по тактике защиты объекта и локализации защищаемых элементов (ПСК-2.2);
- способность разработать комплекс мер по обеспечению информационной безопасности объекта и организовать его внедрение и последующее сопровождение (ПСК-2.3);
- способность организовать контроль защищенности объекта в соответствии с нормативными документами (ПСК-2.4).

3. Место дисциплины в структуре ОП ВО

Дисциплина «Комплексные системы защиты информации на предприятии» относится к базовым. Дисциплина формирует представление о моделировании угроз безопасности информации и процессов защиты информации на предприятии, об особенностях построения комплексной системы защиты информации предприятия и оценка ее эффективности.

Дисциплина изучается на четвертом курсе, требования к входным знаниям, умениям и навыкам определяются требованиями к уровню подготовки по дисциплинам «Аудит защищенности объектов информатизации», «Техническая защита информации», «Моделирование процессов и систем защиты информации».

Изучение дисциплины является основой для освоения последующих дисциплин/практик: «Производственная практика».

4. Объем дисциплины (модуля)

4.1. Объем дисциплины в зачетных единицах с указанием академических (астрономических) часов и виды учебной работы

Виды учебной работы,	Очная форма
Общая трудоемкость в зачетных единицах	7
Общая трудоемкость в часах	252
Аудиторные занятия в часах, в том числе:	62
Лекции	24
Практические занятия	-
Лабораторные занятия	38
Самостоятельная работа в часах	154
Форма промежуточной аттестации	экзамен

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	24
Практические занятия	-
Лабораторные занятий	38
Консультации	0,9
Зачет/зачеты	-
Экзамен/экзамены	36
Курсовые работы	-
Курсовые проекты	–
Всего	98,9

5.Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием количества часов и видов занятий

5.1 Тематический план учебной дисциплины

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
1.	Введение. Основные руководящие документы и показатели эффективности системы защиты информации.	22	2	4	16
2.	Комплексный подход к обеспечению информационной безопасности объекта.	22	2	4	16
3.	Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них.	22	2	4	16
4.	Формирование концепции обеспечения информационной безопасности.	24	4	4	16
5.	Решения по защите информации и оценка их качества. Анализ риска. Общие положения и характеристика атаки на автоматизированную систему.	26	4	4	18
6.	Угрозы информационной безопасности и оценка вероятности их реализации.	26	4	4	18
7.	Формирование облика нарушителя.	24	2	4	18

№ п/п	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекции	Лабораторные	
8.	Алгоритм проведения анализа информационного риска на предприятии.	24	2	4	18
9.	Аналитические технологии управления информационной безопасности. Обеспечение информационной безопасности в чрезвычайных ситуациях. План обеспечения информационной безопасности предприятия.	26	2	6	18
Экзамен		36			
Всего:		**252**	**24**	**38**	**154**

5.2. Содержание:

1. Введение. Основные руководящие документы и показатели эффективности системы защиты информации.

Характеристика "Общих критериев оценки безопасности информационных технологий ISO/IEC 15408". Иерархия показателей эффективности системы защиты информации. Обобщенный методический подход к обеспечению информационной безопасности.

2. Комплексный подход к обеспечению информационной безопасности объекта.

Основные принципы, требования и рекомендации по обеспечению информационной безопасности предприятия. Методика построения (аналитического обследования) системы информационной безопасности предприятия**.**

3. Методика выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них.

Формирование списка сведений, подлежащих защите. Формирование списка организаций и частных лиц, которые могут быть заинтересованы в доступе к охраняемой информации.

4. Формирование концепции обеспечения информационной безопасности.

Информационно-логическая модель объекта защиты. Характеристика основных элементов систем обеспечения информационной безопасности. Рекомендуемая структура концепции обеспечения информационной безопасности**.**

5. Решения по защите информации и оценка их качества. Анализ риска. Общие положения и характеристика атаки на автоматизированную систему.

Метод последовательных уступок. Метод анализа иерархий. Метод экспертных оценок. Общие положения анализа риска. Факторы, влияющие на уровень риска. Характеристика подготовительного этапа нарушения информационной безопасности. Характеристика этапа реализации атаки.

6. Угрозы информационной безопасности и оценка вероятности их реализации.

Иерархия угроз информационной безопасности. Оценка уязвимости информационных ресурсов.

7. Формирование облика нарушителя.

Общая характеристика модели нарушителя. Структура и основные элементы модели нарушителя. Алгоритм формирования облика нарушителя.

8. Алгоритм проведения анализа информационного риска на предприятии.

Оценка возможного ущерба (потерь). Алгоритм проведения анализа информационного риска на предприятии. Стратегия управления рисками. Проверка системы защиты информации.

9. Аналитические технологии управления информационной безопасности. Обеспечение информационной безопасности в чрезвычайных ситуациях. План обеспечения информационной безопасности предприятия.

Информационное обеспечение администратора безопасности. Автоматизация управления информационной безопасностью. Анализ соответствия техническим требованиям. Анализ системного аудита. Классификация чрезвычайных ситуаций. Определение угроз информационной безопасности в чрезвычайных ситуациях. Разработка мер противодействия чрезвычайным ситуациям. Место и роль плана защиты в системе информационной безопасности. Организация планирования. Основные элементы плана защиты и их содержание.

6. Методические материалы для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы.

Обучающемуся важно помнить, что лекция эффективно помогает ему овладеть программным материалом благодаря расстановке преподавателем необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации. Кроме того, во время лекции имеет место прямой визуальный и эмоциональный контакт обучающегося с преподавателем, обеспечивающий более полную реализацию воспитательной компоненты обучения.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков применения методов формирования, организации и поддержки комплекса мер по обеспечению информационной безопасности объекта защиты;
- совершенствование навыков поиска публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем и учитываются при аттестации студента.

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема) дисциплины	Задание	Методические рекомендации по выполнению задания	Форма контроля
1	2	3	4	5
1.	Тема № 1	Усвоить	1. Изучить основные руководящие документы по защите информации.	Контрольный опрос

			2. Изучить показатели эффективности системы защиты информации. Литература основная [1-3]. Дополнительная литература [1-2].	
2.	Тема № 2	Усвоить, приобрести навык	1. Изучить комплексный подход к обеспечению информационной безопасности объекта. Литература основная [1-3]. Дополнительная литература [1-2].	Контрольный опрос
3.	Тема № 3	Усвоить, приобрести навык	1. Изучить методику выявления сведений, представляющих интеллектуальную собственность, и организаций, заинтересованных в них. Литература основная [1-3]. Дополнительная литература [1-2].	Проверка выполнения лабораторной работы
4.	Тема № 4	Усвоить, приобрести навык	1. Изучить формирование концепции обеспечения информационной безопасности. Литература основная [1-3]. Дополнительная литература [1-2].	Контрольный опрос
5.	Тема № 5	Усвоить, приобрести навык	1. Изучить решения по защите информации и оценка их качества. 2. Анализ риска. 3. Общие положения и характеристика атаки на автоматизированную систему. Литература основная [1-3]. Дополнительная литература [1-2].	Контрольный опрос
6.	Тема № 6	Усвоить, приобрести навык	1. Изучить угрозы информационной безопасности и оценку вероятности их реализации. Литература основная [1-3]. Дополнительная литература [1-2].	Контрольный опрос
7.	Тема № 7	Усвоить, приобрести навык	1. Изучить формирование облика нарушителя. Литература основная [1-3]. Дополнительная литература [1-2].	Контрольный опрос
8.	Тема № 8	Усвоить, приобрести навык	1. Изучить алгоритм проведения анализа информационного риска на предприятии. Литература основная [1-3]. Дополнительная литература [1-2, 4].	Контрольный опрос
9.	Тема № 9	Усвоить, приобрести навык	1. Изучить аналитические технологии управления информационной безопасности. 2. Изучить обеспечение информационной безопасности в чрезвычайных ситуациях. 3. Изучить план обеспечения информационной безопасности предприятия. Литература основная [1-3]. Дополнительная литература [1-4].	Контрольный опрос

Формой отчетности по данной дисциплине является экзамен. Необходимые условия допуска к экзамену:

- Наличие полного конспекта лекций.
- Сдача всех лабораторных работ с положительным результатом.

6.2. Тематика и задания для практических занятий (*при наличии*)

Не предусмотрены

6.3. Тематика и задания для лабораторных занятий

1. Построение описания объекта информатизации. Общее описание объекта и его планировка.
2. Построение описания объекта информатизации. Организационная структура предприятия и экспликация помещений отделов.
3. Построение описания объекта информатизации. Перечень и характеристики информационных ресурсов.
4. Построение описания объекта информатизации. Список и характеристики персонала.
5. Проектирование корпоративной сети передачи данных. Список и характеристики средств хранения, обработки, передачи и представления информации.
6. Проектирование корпоративной сети передачи данных. Список и характеристики средств защиты информации.
7. Проектирование корпоративной сети передачи данных. Топология КСПД и схема адресации.
8. Разработка слоев «информационные ресурсы», «КСПД», «персонал», «уязвимости», «угрозы» на плане объекта.
9. Разработка слоев СЗИ на плане объекта.

7. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

а) Основная литература:

1. Комплексная защита информации в корпоративных системах: Учебное пособие / В.Ф. Шаньгин. - М: ИД ФОРУМ: НИЦ ИНФРА-М, 2013. - 592 с. ISBN 978-5-8199-0411-4 Режим доступа: http://znanium.com/catalog.php?bookinfo=402686
2. Интеллектуальные системы защиты информации: учеб, пособие/ Васильев В.И. - 2-е изд., испр. и доп. - М.: Машиностроение, 2013. 172 с. http://www.studentlibrary.ru/book/ISBN9785942756673.html
3. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс,- 474 с. http://www.studentlibrary.ru/book/ISBN9785940746478.htrnl

б) Дополнительная литература:

1. Бизнес-безопасность / Кузнецов И.Н. - М. : Дашков и К, 2012. 416 с. http://www.studentlibran-.ru/book/ISBN9785394014383.html
2. Офисный шпионаж / Мелтон К., Пилиджан К., Сверчински Д. - М. : Альпина Паблишер, - 182 с. http://www.studentlibrary.ru/book/ISBN9785916712070.html .
3. Моделирование процессов управления и принятия решений в условиях чрезвычайных ситуаций / Ямалов И.У. - М. : БИНОМ, 2015. 291 с. http://www.studentlibrary.ru/book/ISBN9785996325627.html
4. Искусство управления информационными рисками / Астахов А.М. - М. : ДМК Пресс, 2010. - 312 с. http://www.studentlibrary.ru/book/ISBN9785940745747.html

в) Периодические издания :

1. «Журнал сетевых решений/LAN» -Режим доступа: http://www.osp.ra/lan/current ;
2. Электронный журнал «Корпоративные сети передачи данных» -Режим доступа: http://www.delpress.ru/

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

Информационно-образовательные ресурсы:
1. www.atlas.Krasnodar.ru -КФ НТЦ «Атлас»: защита информации.
2. ИНТУИТ. Национальный открытый университет - Режим доступа: http://www.intuit.ru/

Электронные библиотечные системы:
1. Университетская библиотека онлайн http://biblioclub.ru
2. «Лань» http://e.lanbook.com/
3. ЭБС «Znanium»
4. Справочно-информационная система (СИС) «Гарант».
5. Справочно-информационная система «Консультант».
6.Электронно-библиотечная система (ЭБС) «Инфра-М».

9. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционная аудитория, оснащенная проектором, компьютером.
Лаборатория с ПЭВМ на каждого студента.
Лаборатория технической защиты информации.
Лаборатория технических средств охраны и видеонаблюдения.