Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Костромской государственный университет»

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки *«(09.03.02) Информационные системы и технологии»*

Все направленности

Квалификация (степень) выпускника: *бакалавр*

Кострома
2020

Рабочая программа дисциплины «Информационная безопасность» разработана в соответствии с Федеральным государственным образовательным стандартом по направлению 09.03.02 Информационные системы и технологии (уровень бакалавриата), утвержден приказом Министерства образования и науки РФ № 926 от 19.09.17.

Разработал:  Дружинина А.Г., к.т.н., доцент

Рецензент:  Кириллова Е.С, доцент каф. ИВТ, к.т.н., доцент

Директор Института автоматизированных систем и технологий

Лустгартен Ю.Л., к.т.н., доцент

подпись

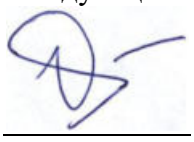
УТВЕРЖДЕНО:

На заседании кафедры Информационных систем и технологий
Протокол заседания кафедры № 8 от 26.05.2020 г.
Заведующий кафедрой Информационных систем и технологий

Киприна Л.Ю., к.т.н., доцент

Подпись

На заседании кафедры Информатики и вычислительной техники
Протокол заседания кафедры №10 от 20 июня 2020 г.
Заведующий кафедрой Информатики и вычислительной техники



Денисов А.Р., д.т.н., доцент

Подпись

1. Цели и задачи освоения дисциплины

Цель дисциплины:

получение компетенций в области решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности

Задачи дисциплины:

–получение студентами знаний в области требований нормативно-правовых документов, регламентирующих отношения в сфере деятельности по защите конфиденциальной информации в, том числе защите государственной тайны, а также в области требований Российских и международных стандартов по информационной безопасности;

–знакомство с организационными и техническими мероприятиями, обеспечивающими эффективность защиты информации в области обеспечения целостности и доступности конфиденциальной информации;

–знакомство с возможными нарушениями в сфере компьютерной безопасности и приобретение навыков моделирования угроз для расчета обеспечения условий безопасности;

–приобретение практических навыков защиты информации на современных предприятиях с использованием шифровальных (криптографических) средств.

2. Перечень планируемых результатов обучения по дисциплине

В результате освоения дисциплины обучающийся должен:

освоить компетенции:

ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Код и содержание индикаторов компетенции:

ОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3.3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.

знать:

– основы законодательства РФ в области информационной безопасности;

– основные положения стандартов РФ в области обеспечения целостности и доступности информации;

– подходы к моделированию угроз информационной безопасности;

– правила применения средств защиты (в т.ч. криптографических);

– основы криптографии;

– подходы к построению систем защиты современного предприятия;

– основы законодательства в области защиты персональных данных.

уметь:

– выбирать средства защиты (программно-, аппаратно- или программно-аппаратно-) под конкретные задачи;

– разрабатывать модель угроз информационной безопасности;

– применять криптографические средства защиты информации;

– разрабатывать руководящие документы по защите информации.

владеть:

– навыками работы с нормативно-правовой документацией в области информационной безопасности;

– навыками работы с инструментами поиска проблем для обоснования принятых подходов к обеспечению информационной безопасности;

– навыками работы с криптографическими средствами защиты информации.

3. Место дисциплины в структуре ОП ВО

Дисциплина относится в обязательную часть Блока 1. Изучается в 6 семестре.

Изучение дисциплины основывается на ранее освоенных дисциплинах/практиках: информатика и информационные технологии, сети и телекоммуникации.

Изучение дисциплины является основой для освоения последующих дисциплин/практик: основы информатизации предприятий, практика по получению профессиональных умений и опыта профессиональной деятельности.

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	5
Общая трудоемкость в часах	180
Аудиторные занятия в часах, в том числе:	64
Лекции	32
Лабораторные занятия	32
Самостоятельная работа в часах	80+36
Форма промежуточной аттестации	Экзамен

4.2. Объем контактной работы на 1 обучающегося

Виды учебных занятий	Очная форма
Лекции	32
Лабораторные занятий	32
Консультации	
Экзамен	2,35
Всего	66,35

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

5.1 Тематический план учебной дисциплины

№	Название раздела, темы	Всего з.е/час	Аудиторные занятия		Самостоятельная работа
			Лекц.	Лаб.	
1	Введение. Проблематика и основные понятия	9	2	2	5
2	Конфиденциальность информации	9	2	2	5
3	Целостность информации	9	2	2	5
4	Доступность информации	9	2	2	5
5	Источники угроз. Классификация и обзор	9	2	2	5
6	Источники угроз. Инсайдеры	9	2	2	5
7	Модели и концепции построения систем защиты	9	2	2	5
8	Криптография. Основные понятия.	9	2	2	5
9	Криптография. PKI и TLS-SSL	9	2	2	5
10	Электронная подпись	9	2	2	5
11	Сетевые атаки и сетевая безопасность	9	2	2	5
12	Целенаправленные атаки APT	9	2	2	5
13	Разведка на основе открытых источников OSSINT	9	2	2	5
14	Государственная политика в области ИБ	9	2	2	5
15	Защита ИСПДн на предприятии	9	2	2	5
16	Защита коммерческой тайны на предприятии	9	2	2	5
17	Подготовка к экзамену	36			36
	Итого:	**5/180**	**32**	**32**	**80+36**

5.2. Содержание:

1. Введение. Проблематика и основные понятия. Понятия информационный актив, стейкхолдер, риск, угроза.
2. Методы и средства обеспечения конфиденциальности информации.
3. Методы и средства обеспечения целостности информации.
4. Методы и средства обеспечения доступности информации.
5. Источники угроз информации. Классификация и обзор основных источников угроз. Антропогенные и не антропогенные угрозы.
6. Источники угроз информации. Инсайдеры, как самый опасный источник угроз.
7. Модели и концепции построения систем защиты. Формальные модели доступа – дискреционная и мандатная. Концепции построения систем защиты – «zero trust», «kill chain» и SASE (Secure Access Service Edge).
8. Криптография. Основные понятия. Криптосистемы симметричные и асимметричные. Криптографические хэш функции.
9. Криптография. Архитектура инфраструктуры открытых ключей PKI. Защищенный сетевой доступ и протокол TLS-SSL.
10. Электронная подпись. Принципы функционирования. Государственное регулирование.
11. Сетевые атаки и сетевая безопасность. Основные сетевые атаки и методы защиты.
12. Целенаправленные атаки APT. Методы защиты и концепция UEBA (User Entity Behavior Analytics).
13. Разведка на основе открытых источников OSSINT (Open source intelligence). Основные принципы. Источники открытой информации.
14. Государственная политика в области ИБ. Обзор законодательства.
15. Защита ИСПДн на предприятии. Основные принципы. Законодательство. Алгоритм действий.
16. Защита коммерческой тайны на предприятии. Основные принципы. Законодательство. Алгоритм действий.

6. Методические материалы для обучающихся по освоению дисциплины

6.1. Самостоятельная работа обучающихся по дисциплине (модулю)

№ п/п	Раздел (тема) дисциплины	Задание	Часы	Методические рекомендации по выполнению задания	Форма контроля
1	Введение. Проблематика и основные понятия	Изучить материалы лекции и рекомендованной литературы.	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, заслушивание и обсуждение докладов
2	Конфиденциальность информации	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
3	Целостность информации	Изучить материалы лекции и рекомендованной	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы

		литературы Создание отчета по лабораторной работе			
4	Доступность информации	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
5	Источники угроз. Классификация и обзор	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
6	Источники угроз. Инсайдеры	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
7	Модели и концепции построения систем защиты	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
8	Криптография. Основные понятия.	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
9	Криптография. PKI и TLS-SSL	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
10	Электронная подпись	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
11	Сетевые атаки и сетевая безопасность	Изучить материалы лекции и рекомендованной литературы	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы

		Создание отчета по лабораторной работе			
12	Целенаправленные атаки APT	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
13	Разведка на основе открытых источников OSSINT	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
14	Государственная политика в области ИБ	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
15	Защита ИСПДн на предприятии	Изучить материалы лекции и рекомендованной литературы Создание отчета по лабораторной работе	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
16	Защита коммерческой тайны на предприятии	Изучить материалы лекции и рекомендованной литературы	5	Использовать материалы лекции и рекомендованной литературы	Устный опрос, защита лаб. работы
17	Подготовка к экзамену	Изучить материалы лекции и рекомендованной литературы	36	Использовать материалы лекции и рекомендованной литературы	Экзамен

6.2. Тематика и задания для лабораторных занятий

1	Аудит активов предприятия и формирование требований к защите
2	Средства защиты в локальных сетях ACL
3	Средства защиты в локальных сетях VLAN и AAA
4	DLP. Выявление и анализ каналов утечек
5	DLP. Разработка правил
6	Выбор средств защиты для предприятия
7	Firewall OPN Sence
8	GPG
9	SNORT и NMAP

10	SNORT и Metasploit
11	Анализ требований законодательства в области защиты КТ
12	Анализ требований законодательства в области защиты ГИС
13	Разработка системы защиты ИСПДн на предприятии
14	Разработка системы защиты КТ на предприятии

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

Основная литература

1. Спицын, В.Г. Информационная безопасность вычислительной техники : учебное пособие / В.Г. Спицын ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР).-Томск : Эль Контент, 2011.-148 с. : ил.,табл., схем. - ISBN 978-5-4332-0020-3; Тоже [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=208694
2. Загинайлов, Ю.Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов.-Москва ; Берлин : Директ-Медиа,2015. -253 с. : ил. - Библиогр. в кн.- ISBN 978-5-4475-3946-7 ; То же [Электронный ресурс].-URL:http://biblioclub.ru/index.php?page=book&id=276557

Дополнительная литература

3. Артемов, А.В. Информационная безопасность : курс лекций / А.В.Артемов ; Межрегиональная Академия безопасности и выживания.-Орел : МАБИВ, 2014.-257 с. : табл., схем. ; То же [Электронный ресурс]. -URL: http://biblioclub.ru/index.php?page=book&id=428605
4. Хаулет, Т. Инструменты безопасности с открытым исходным кодом / Т.Хаулет. -2-е изд.,испр.-Москва : Национальный Открытый Университет «ИНТУИТ», 2016. 566 с. : ил.-(Основы информационных технологий).-ISBN 978-5-94774-629-7 ; То же [Электронный ресурс]. -URL: http://biblioclub.ru/index.php?page=book&id=429025
5. Заика, А. Компьютерная безопасность / А.Заика. -Москва : РИПОЛ классик, 2013.-160 с. -(Компьютер —это просто).-ISBN 978-5-386-06476-1 ; То же [Электронный ресурс].-URL:http://biblioclub.ru/index.php?page=book&id=227317
6. Технологии защиты информации в компьютерных сетях / Н.А.Руденков, А.В. Пролетарский, Е.В. Смирнова, А.М. Суровов. -2-е изд., испр.-Москва : Национальный Открытый Университет «ИНТУИТ», 2016.-369 с. : ил. ; То же [Электронный ресурс].-URL: http://biblioclub.ru/index.php?page=book&id=428820
7. Петров, А. А. Компьютерная безопасность : Криптографические методы защиты / А. А. Петров. -М. : ДМК, 2000.-448 с. : ил. -([Информационные технологии для инженеров]).-Библиогр.:3 с. 437-445.-ISBN 5-89818-064-8
8. Девянин, П. Н. Модели безопасности компьютерных систем : Учеб. пособие для студ. высш. учеб. заведений / П. Н. Девянин.-М. : Академия, 2005.-144 с.- (Высшее профессиональное образование).- (Информационная безопасность). - Библиогр.: с. 139-140. -ISBN 5-7695-2053-1

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

Информационно-образовательные ресурсы:

1. Национальный открытый университет ИНТУИТ: URL: *http://www.intuit.ru*
2. Информационный портал по безопасности: URL: *http:/www.securitylab.ru*;
3. Сайт ИТ-специалистов-блогеров:URL: *http://www.habr.com*

Электронные библиотечные системы:

1. ЭБС «Лань»
2. ЭБС «Университетская библиотека online»
3. ЭБС «Znanium»

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

Для проведения всех видов занятий по дисциплине необходимо следующее материально-техническое обеспечение:

№ п/п	**Специализированные аудитории и классы**	Номер аудитории
1	Аудитория, оборудованная мультимедиа, для лекций	Е-326, Е-226
2	Компьютерные классы	Е-327, Е-320
Учебное оборудование		
	Персональные компьютеры, объединенные в локальную сеть, с выходом в Интернет	
№ п/п	**Программное обеспечение**	
1	MS Windows (Dream Spark Premium), Linux	Е-327
2	Офисный пакет	Е-327, Е-320
3	Симулятор вычислительной сети	Е-327, Е-320
4	VirtualBox	Е-327, Е-320