Федеральное государственное бюджетное образовательное учреждение высшего образования
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ИНСТИТУТ ЭКОНОМИКИ, МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И АНАЛИЗА ДАННЫХ
ОТДЕЛЕНИЕ ПРИКЛАДНОЙ ИНФОРМАТИКИ

кафедра системного анализа и информатики

УТВЕРЖДЕНА

решением кафедры Системного анализа и информатики

Протокол №6 от «2» сентября 2019г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Б1.О.10.05 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

направление подготовки
09.03.03 Прикладная информатика
направленность (профиль)
«Прикладная информатика в энергетических системах»
квалификация
бакалавр
очно-заочная форма обучения

Год набора – 2019

Москва, 2019 г.

Автор–составитель: к.т.н., доцент
кафедра Системного анализа и информатики Каширская Е.Н.

Заведующий кафедрой
Системного анализа и информатики Маруев С.А

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы
2. Объем и место дисциплины в структуре ОП ВО
3. Содержание и структура дисциплины
4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине
4.1. Формы и методы текущего контроля успеваемости.
4.2. Материалы текущего контроля успеваемости обучающихся
4.3. Оценочные средства для промежуточной аттестации
4.4. Методические материалы
5. Методические указания для обучающихся по освоению дисциплины
5.1. Методические указания по вопросам на понимание лекционного материала
5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов
5.3.Методические рекомендации по подготовке к экзамену по дисциплине
6. Учебная литература и ресурсы информационно-телекоммуникационной сети «Интернет», включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине
6.1. Основная литература.
6.2. Дополнительная литература.
6.3. Учебно-методическое обеспечение самостоятельной работы.
6.4. Нормативные правовые документы
6.6. Иные источники.
7. Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения программы

1.1. Дисциплина «Информационная безопасность» обеспечивает овладение следующими компетенциями:

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	Способность разработать проект на основе оценки ресурсов и ограничений	УК ОС-2.1	Способность к самоопределению по типу участия в различных типах проектов (на основе полученного в школе опыта)
		УК ОС-2.2	Способность определять и оценивать ресурсы и существующие ограничения проекта с качественной и количественной точек зрения
ОПК-3	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1	Способность анализировать и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-4	Способность участвовать в разработке стандартов, норм и правил, а также технической документации, связанной с профессиональной деятельностью;	ОПК-4.1	способен разработывать стандарты, нормы и правила, при использовании ИС
		ОПК-4.2	Способен использовать техническую документацию, связанную с профессиональной деятельностью;

1.2.В результате освоения дисциплины у студентов должны быть сформированы:

ОТФ/ТФ (при наличии профстандарта)	Код этапа освоения компетенции	Результаты обучения
- разработка проекта с учетом ресурсов и ограничений	УК ОС-2.1; УК ОС-2.2	на уровне знаний: знать способы оценки ресурсов и ограничений.
		на уровне умений: уметь опираться на имеющиеся ресурсы и ограничения при разработке проектов
		на уровне навыков: разрабатывать проекты информационных систем с учетом имеющихся ресурсов и наложенных ограничений
- решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ОПК-3.1	на уровне знаний: знать задачи в области профессиональной деятельности и требования информационной безопасности;
		на уровне умений: решать стандартные задачи на основе информационной культуры и применять информационные технологии;
		на уровне навыков: владеть способами решения стандартных задач и информационными технологиями.
-проектировать информационные системы в соответствии с профилем подготовки	ОПК-4.1 ОПК-4.2	на уровне знаний: знать методы и средства проектирования информационных систем;
		на уровне умений: пользоваться своими знаниями для проектирования информационных систем
		на уровне навыков: проектировать информационные системы и структуры баз данных;

2. Объем и место дисциплины в структуре ОП ВО

Объем дисциплины

Объем дисциплины в ЗЕ и академических/астрономических часах – 6 ЗЕ (216/162 ч).
Количество академических/астрономических часов, выделенных на очно--заочной форме обучения на контактную работу– 48/36 часов (в т.ч. лекц. - 16 ч., практ.-32 ч.); на самостоятельную работу обучающихся– 132/99часов, экзамен – 36/27 ч.

Место дисциплины в структуре ОП ВО

Дисциплина Б1.О.10.05 «Информационная безопасность» относится к обязательной части учебного плана по направлению подготовки 09.03.03 Прикладная информатика.
Дисциплина изучается на 3 курсе в 6 семестре (очно-заочная форма обучения).
Дисциплины опирается на объём знаний, полученных при изучении таких дисциплин, как Информатика, Программирование и алгоритмизация, Математический анализ, Линейная алгебра, Операционные системы, Теория вероятностей.
Форма промежуточной аттестации – экзамен.

3. Содержание и структура дисциплины

Очно-заочная форма обучения

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 1	Актуальность информационной безопасности в современных условиях	19	1		2		16	Д, О
Тема 2	Угрозы и возможные каналы утечки конфиденциальной информации.	19	1		2		16	Д, О
Тема 3	Компьютерные вирусы и деструктивные программы.	19	1		2		16	Д, О
Тема 4	Методы защиты информации в автоматизированных системах обработки данных.	36	4		8		24	Д, О
Тема 5	Стандарты безопасности компьютерных систем.	36	4		8		24	Д, О
Тема 6	Обеспечение информационной безопасности в Интернет.	20	2		4		14	Д, О

№ п/п	Наименование тем (разделов)	Объем дисциплины, час.						Форма текущего контроля успеваемости*, промежуточной аттестации
		Всего	Контактная работа обучающихся с преподавателем по видам учебных занятий				СР	
			Л	ЛР	ПЗ	КСР		
Тема 7	Сеть интранет как основной объект нападений из Интернет.	31	3		6		22	Д, О
Промежуточная аттестация		36						экзамен
Всего академ./астроном.часов:		**216/162**	**16/12**		**32/24**		**132/99**	**36/27**

Примечание: * – формы текущего контроля успеваемости: доклад(ы) (Д), опрос (О).

Содержание дисциплины

Тема 1. Актуальность информационной безопасности в современных условиях.
1.1. Что такое информационная безопасность.
1.2. Актуальность проблемы информационной безопасности.
1.3. Понятия и определения в информационной безопасности.

Тема 2. Угрозы и возможные каналы утечки конфиденциальной информации.
2.1. Основные закономерности возникновения и классификация угроз информационной безопасности.

2.2. Пути и каналы утечки информации и их обобщенная модель.
2.3. Классификация каналов утечки информации.
Тема 3. Что такое компьютерные вирусы и как они работают.
3.1. Классификация компьютерных вирусов.
3.2. Файловые вирусы.
3.3. Загрузочные вирусы.
3.4. Макровирусы.
3.5. Сетевые вирусы.
3.6. Прочие вредные программы.

Тема 4. Методы обнаружения и удаления компьютерных вирусов.
4.1. Откуда берутся компьютерные вирусы.
4.2. Основные правила защиты от компьютерных вирусов.
4.3. Антивирусные программы.
4.4. Восстановление пораженных компьютерными вирусами объектов.

Тема 5. Методы защиты информации в автоматизированных системах обработки данных.
5.1. Краткий обзор современных методов защиты информации.
5.2. Ограничение доступа.
5.3. Контроль доступа к аппаратуре.
5.4. Разграничение и контроль доступа к информации АСОД.
5.5. Разграничение привилегий на доступ.
5.6. Идентификация и установление подлинности объекта.
5.7. Криптографическое преобразование информации.
5.8. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
5.9. Методы и средства защиты информации от случайных воздействий.
5.10. Методы защиты информации от аварийных ситуаций.
5.11. Организационные мероприятия по защите информации.
5.12. Законодательные меры по защите информации.
5.13 Критерии безопасности компьютерных систем. "Оранжевая книга".
5.14. Руководящие документы Гостехкомиссии.

Тема 6. Удаленные атаки на интрасети.
6.1 Примеры взломов сетей и Web-узлов.
6.2 Пользователи и злоумышленники в Internet.
6.3 Причины уязвимости сети Internet.
6.4 Обеспечение информационной безопасности организации при ее подключении к Internet.
6.5 Защита архитектуры клиент/сервер
Тема 7. Интрасеть как основной объект нападений из Internet.
7.1 Удаленные атаки на интрасети.
7.2 Классические методы взлома интрасетей.
7.3 Современные методы взлома интрасетей.
7.4 Улучшение паролей.
7.5 Одноразовые пароли.
7.6 Серверы аутентификации.
7.7 Физическая изоляция.
7.8 Изоляция протокола.
7.9 Выделенные каналы и маршрутизаторы.
7.10 Защита систем управления базами данных.
7.11 Защита в сетевых операционных системах.

4. Материалы текущего контроля успеваемости обучающихся и фонд оценочных средств промежуточной аттестации по дисциплине

4.1. Формы и методы текущего контроля успеваемости.

4.1.1. В ходе реализации дисциплины «Информационная безопасность» используются следующие методы текущего контроля успеваемости обучающихся:

Тема (раздел)	Методы текущего контроля успеваемости
Тема 1	Доклады с презентацией, опрос на практическом занятии
Тема 2	Доклады с презентацией, опрос на практическом занятии
Тема 3	Доклады с презентацией, опрос на практическом занятии
Тема 4	Доклады с презентацией, опрос на практическом занятии
Тема 5	Доклады с презентацией, опрос на практическом занятии
Тема 6	Доклады с презентацией, опрос на практическом занятии
Тема 7	Доклады с презентацией, опрос на практическом занятии

4.1.2. Экзамен проводится в форме устного ответа на билеты (по 2 вопроса в билете).

4.2. Материалы текущего контроля успеваемости обучающихся

Текущий контроль успеваемости осуществляется непрерывно, на протяжении всего курса. Прежде всего, это устный опрос по ходу лекции, выполняемый для оперативной активизации внимания обучающихся и оценки их уровня восприятия. Помимо этого, контроль самостоятельной работы обучающихся осуществляется при опросе на практических занятиях, докладах с презентацией.

Тема 1. Актуальность информационной безопасности в современных условиях

Вопросы для подготовки обучающихся к практическим занятиям

1. Что такое информационная безопасность.
2. Актуальность проблемы информационной безопасности.
3. Понятия и определения в информационной безопасности.

Тема 2. Угрозы и возможные каналы утечки конфиденциальной информации

Вопросы для подготовки обучающихся к практическим занятиям

1. Основные закономерности возникновения и классификация угроз информационной безопасности.
2. Пути и каналы утечки информации и их обобщенная модель.
3. Классификация каналов утечки информации.
4. Типы несанкционированного доступа и условия работы средств защиты.
5. Варианты защиты от локального НСД.

Тема 3. Компьютерные вирусы и деструктивные программы

Вопросы для подготовки обучающихся к практическим занятиям

1. Что такое компьютерные вирусы и как они работают?
2. Классификация компьютерных вирусов.
3. Файловые вирусы.
4. Загрузочные вирусы.
5. Макровирусы.
6. Сетевые вирусы.
7. Прочие вредоносные программы.
8. Методы обнаружения и удаления компьютерных вирусов.
9. Откуда берутся компьютерные вирусы?
10. Основные правила защиты от компьютерных вирусов.
11. Антивирусные программы.
12. Восстановление пораженных компьютерными вирусами объектов

Тема 4. Методы защиты информации в автоматизированных системах обработки данных.

Вопросы для подготовки обучающихся к практическим занятиям

1. Ограничение доступа.
2. Контроль доступа к аппаратуре.
3. Разграничение и контроль доступа к информации.
4. Разграничение привилегий на доступ.
5. Идентификация и установление подлинности объекта.
6. Криптографическое преобразование информации.
7. Защита информации от утечки за счет побочного электромагнитного излучения и наводок.
8. Методы и средства защиты информации от случайных воздействий.
9. Методы защиты информации от аварийных ситуаций.
10. Организационные мероприятия по защите информации.
11. Законодательные меры по защите информации.

Тема 5. Стандарты безопасности компьютерных систем

Вопросы для подготовки обучающихся к практическим занятиям

1. Критерии безопасности компьютерных систем.
2. «Оранжевая книга».
3. Руководящие документы Гостехкомиссии РФ.
4. Европейские критерии безопасности.
5. Государственные (национальные) стандарты безопасности РФ.

Тема 6. Обеспечение информационной безопасности в Интернет

Вопросы для подготовки обучающихся к практическим занятиям

1. Типы несанкционированного доступа и условия работы средств защиты.
2. Вариант защиты от удаленного НСД.
3. Средства защиты операционной системы.
4. Надежность средств защиты.
5. Примеры взломов сетей и Web-узлов.
6. Пользователи и злоумышленники в Интернет.
7. Причины уязвимости сети Интернет.
8. Обеспечение информационной безопасности организации при ее подключении к Интернет.
9. Защита архитектуры клиент/сервер.
10. Защита каналов связи в Интернет.
11. Межсетевые экраны.
12. Шифрование передаваемой информации.
13. Аутентификация в Интернет.
14. Улучшение паролей. «Солёные» пароли.
15. Одноразовые пароли.
16. Серверы аутентификации.
17. Защита электронного обмена данными в Интернет.
18. Сетевое резервное копирование.

Тема 7. Сеть интранет как основной объект нападений из Интернет.

Вопросы для подготовки обучающихся к практическим занятиям

1. Удаленные атаки на сеть интранет.

2. Классические методы взлома сети интранет.
3. Современные методы взлома сети интранет.
4. Защита хостов сети интранет.
5. Защита систем управления базами данных.
6. Защита в сетевых операционных системах.
7. Программно-аппаратные методы и средства ограничения доступа к компонентам компьютера.
8. Выбор сетевой топологии сети интранет.
9. Физическая изоляция сети интранет.
10. Изоляция протокола.
11. Выделенные каналы и маршрутизаторы.

4.3. Оценочные средства для промежуточной аттестации

4.3.1. Формируемые компетенции

Код компетенции	Наименование компетенции	Код этапа освоения компетенции	Наименование этапа освоения компетенции
УК ОС-2	Способность разработать проект на основе оценки ресурсов и ограничений	УК ОС-2.1	Способность к самоопределению по типу участия в различных типах проектов (на основе полученного в школе опыта)
		УК ОС-2.2	Способность определять и оценивать ресурсы и существующие ограничения проекта с качественной и количественной точек зрения
ОПК-3	способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1	Способность анализировать и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
ОПК-4	Способность участвовать в разработке стандартов,	ОПК-4.1	способен разработывать стандарты, нормы и правила, при использовании ИС

	норм и правил, а также технической документации, связанной с профессиональной деятельностью;	ОПК-4.2	Способен использовать техническую документацию, связанную с профессиональной деятельностью;

4.3.2. Типовые оценочные средства

Промежуточный контроль проводится в форме зачета и предусматривает устный ответ на вопросы по билету.

Код и наименование этапа освоения компетенции	Показатель оценивания	Критерий оценивания
УК ОС-2.1 УК ОС-2.2 Разработка проекта информационной системы на основе оценки ресурсов и ограничений	Определяет тип(ы) проекта(ов) для участия в них с учетом личностных, социальных и профессиональных интересов (социальные, направленные на развитие волонтерского движения; профессионально-ориентированные, направленные на самоопределение студентов и др.). Определяет оптимальное количество необходимых для разработки проекта ресурсов Определяет существующие ограничения для реализации проекта Осуществляет оценку по количественным показателям ресурсов	Осуществлен выбор типа проекта и степени (уровня) участия студента в проекте Выражена готовность к сотрудничеству в различных группах (межпредметных) и определена ролевая позиция в группе по осуществлению проектов Оптимально распределены обязанности по задачам и подзадачам в рамках цели проекта Определено оптимальное количество необходимых для разработки проекта ресурсов Определены все возможные ограничения, существующие в рамках реализации проекта Оформлено ресурсное обеспечение проекта и существующие ограничения в электронной форме (использование информационных технологий)

ОПК-3.1 Способность анализировать и решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	Названы основные виды информационного поиска (библиографический, документальный, фактографический, аналитический), приведены их определения, связи между собой и различия Определены условия поиска (цель, предмет, метод, хронологический и географический охват, полнота, интенсивность) Сформулирован общий случай процедуры поиска (уточнена информационная потребность и формулировка запроса, определена совокупность информационных массивов, извлечена информация из массивов, пользователь ознакомлен с полученной информацией) Составлен примерный план поиска по конкретно заданной теме	Знает основные виды информационного поиска Определяет условия поиска Формулирует общий случай процедуры информационного поиска Составляет примерный план поиска применительно к задаваемой преподавателем теме.
ОПК-4.1 ОПК-4.2 Способен разработывать стандарты, нормы и правила, при использовании ИС Способен использовать техническую документацию, связанную с профессиональной деятельностью;	Оценено и аргументировано соответствие области применения задачи Продемонстрировано влияние положений НПА или стандартов на решение прикладной задачи. Приведены примеры направлений развития современных ИКТ в выбранной области Продемонстрировано на базовом уровне владение каким-либо программным обеспечением в выбранной области	Оценивает соответствие содержимого НПА или стандартов области применения задачи Демонстрирует применение в рамках учебного примера найденных данных в решении прикладной задачи

Перечень вопросов к экзамену

1. Базовые принципы безопасности операционных систем.
2. Развитие политики безопасности в Windows и ее будущее.
3. Общая структура Windows XP и методы атак.
4. Пароли и распределение прав пользователей.
5. Система прав доступа.
6. Политика паролей.
7. Построение защищенной файловой системы.
8. Файловая система и права доступа.
9. Шифрование файлов и папок.
10. Настройки папок.
11. Альтернативные оболочки.
12. Обеспечение защиты операционных систем от атак по компьютерным сетям и Интернету.
13. Сетевая защита и брандмауэр.
14. Удаленные сеансы пользователей.
15. Внутренняя политика безопасности операционных систем семейства Windows
16. Реестр. Политика безопасности.
17. Политика обновления.
18. Получение информации о процессах, происходящих в системе.
19. Аудит событий.
20. Просмотр событий.
21. Диспетчер задач и внутренние параметры системы.
22. Восстановление поврежденной системы.
23. Точки восстановления.
24. Консоль восстановления.
25. Загрузочное меню.
26. Наиболее распространенные угрозы.
27. Законодательный уровень информационной безопасности.
28. Стандарты и спецификации в области информационной безопасности.
29. Административный уровень информационной безопасности.
30. Управление рисками.
31. Процедурный уровень информационной безопасности.
32. Основные программно-технические меры.
33. Идентификация и аутентификация, управление доступом.
34. Протоколирование и аудит, шифрование, контроль целостности.
35. Экранирование, анализ защищенности.
36. Обеспечение высокой доступности.
37. Тунелирование и управление.
38. Международные стандарты информационного обмена.
39. Понятие угрозы.
40. Информационная безопасность в условиях функционирования в России глобальных сетей.
41. Виды противников или «нарушителей».
42. Виды вирусов.
43. Три вида возможных нарушений информационной системы. Защита от нарушений.
44. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
45. Основные положения теории информационной безопасности информационных систем.

46. Модели безопасности и их применение.
47. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование.
48. Анализ способов нарушений информационной безопасности.
49. Использование защищенных компьютерных систем.
50. Методы криптографии.
51. Основные технологии построения защищенных ИС.
52. Место информационной безопасности экономических систем в национальной безопасности страны.
53. Концепция информационной безопасности
54. Политики аудита.
55. Распространённые методы НСД в сетях.
56. Типовая структура антивирусной системы предприятия.
57. Государственное регулирование деятельности в области защиты информации.
58. Сертификация программного обеспечения и оборудования.
59. Симметричные криптосистемы.
60. Криптография с открытым ключом.

4.4. Методические материалы

4.4.1. Методические материалы, определяющие процедуру оценивания ответов обучающихся на вопросы на понимание лекционного материала

Критериями оценки ответа обучающихся на лекционном занятии выступают:

- правильность ответов на вопросы преподавателя по изученному материалу;
- полнота и лаконичность ответа;
- степень понимания тематики предмета;
- логика и аргументированность изложения материала;
- приведение примеров, демонстрирующих умение и владение полученными знаниями по темам предмета в раскрытии поставленных вопросов.

4.4.2. Методические материалы, определяющие процедуру оценивания при проведении опроса на практическом занятии

Оценки **«отлично»** заслуживает обучающийся, обнаруживший всестороннее, систематическое и глубокое знание вопроса, умение свободно ориентироваться в теме, усвоивший основную, и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка «отлично» выставляется обучающимся, усвоившим взаимосвязь основных понятий в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала;

Оценки **«хорошо»** заслуживает обучающийся, обнаруживший полное знание темы, успешно выполняющий предусмотренные программой задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка «хорошо» выставляется обучающимся, показавшим систематический характер знаний по пройденному материалу и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебы и профессиональной деятельности;

Оценки **«удовлетворительно»** заслуживает обучающийся, обнаруживший знание основного материала в объеме, необходимом для дальнейшего усвоения материала и предстоящей работы по профессии, знакомый с основной литературой, рекомендованной программой.

Оценка **«неудовлетворительно»** выставляется обучающемуся, обнаружившему пробелы в знаниях основного материала темы, допустившему принципиальные ошибки в понимании и изложении учебного материала.

4.4.3.Методические материалы, определяющие процедуру оценивания промежуточной аттестации по дисциплине

Экзамен принимается в устной форме, по билетам. Задание для экзамена включает два теоретических вопроса. Оценка знаний обучающегося на экзамене носит комплексный характер и определяется его:

- ответом на экзамене;
- учебными достижениями в семестровый период.

Знания, умения, навыки обучающегося на зачете оцениваются оценками: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Основой для определения оценки служит уровень усвоения обучающимися материала, предусмотренного данной рабочей программой.

Оценивание студента на экзамене по дисциплине «Информационная безопасность»

Оценка	Требования к знаниям
Отлично	«Отлично» выставляется обучающемуся, если он показал полные, глубокие и систематические знания, знакомство с основной и дополнительной литературой, полный и правильный ответ, творческий подход в понимании и изложении учебного материала, полное выполнение мероприятий текущего контроля.
Хорошо	«Хорошо» выставляется обучающемуся, если он показал достаточные и систематизированные знания, знакомство с основной и отчасти с дополнительной литературой, дал в целом правильный ответ, показал понимание и изложении учебного материала, полностью выполнил мероприятий текущего контроля. Допустимы погрешности при выполнении мероприятий промежуточного контроля и при ответе.
Удовлетвори тельно	«Удовлетворительно» выставляется обучающемуся, если он выполнил не все предусмотренные программой задания, не полностью отработал практические или лабораторные занятия, необходимые дополнительные занятия по соответствующей дисциплине, допустил непринципиальные ошибки при ответе. Допустимо знание основного учебного материала в минимальном объеме, необходимом для дальнейшей учебы и работы, имеются погрешности при выполнении мероприятий промежуточного контроля и при ответе.
Недовлетвори тельно	«Неудовлетворительно» выставляется обучающемуся, если он не выполнил предусмотренные программой задания, не отработал практические или лабораторные занятия, необходимые дополнительные занятия по соответствующей дисциплине, нарушил академические нормы, имеет существенные погрешности при выполнении мероприятий текущего контроля, допущены существенные ошибки при ответе, необходима некоторая дополнительная работа.

5. Методические указания для обучающихся по освоению дисциплины (модуля)

5.1. Методические указания по вопросам на понимание лекционного материала

На лекциях рекомендуется слушать предлагаемый лектором материал, при этом параллельно конспектировать основные положения, поскольку это дает наибольший результат в усвоении материала. Предоставляется возможность задавать вопросы на уточнение понимания темы и принимать участие в ее обсуждении.

Кроме этого, для лучшего освоения материала и систематизации знаний по дисциплине, необходимо постоянно разбирать материалы лекций по конспектам и учебным пособиям. Во время самостоятельной проработки лекционного материала особое внимание следует уделять возникшим вопросам, непонятным терминам, спорным точкам зрения. Все такие моменты следует выделить или выписать отдельно для дальнейшего обсуждения на практическом занятии. В случае необходимости следует обращаться к преподавателю за консультацией. Полный список литературы по дисциплине приведен в разделе 6 настоящей программы.

5.2. Методические указания по подготовке вопросов для самостоятельного изучения к занятиям практического (семинарского) типов

Подготовка обучающегося к практическому занятию осуществляется на основании плана раскрытия темы практического занятия, которое разрабатывается преподавателем на основе рабочей программы и доводится до сведения обучающегося своевременно.

При подготовке к практическому занятию обучающемуся необходимо изучить внимательно основные вопросы темы семинара. Важным условием успешной подготовки к практическому занятию является четкая организация самостоятельной работы студентов по изучению учебной и дополнительной литературы. Умение анализировать и применять для ответов на вопросы и решения задач и заданий полученные знания при самостоятельной подготовке в значительной степени определяет успешность освоения материала по дисциплине и формирование у обучающихся соответствующих компетенций.

Подготовка вопросов для самостоятельного изучения включает: изучение необходимой литературы (обязательной, дополнительной литературы, специальных периодических изданий, Интернет-ресурсов), подготовку конспекта ответа, ответы на вопросы.

При подготовке к практическим занятиям важно:

- использовать достаточно широкий диапазон массива информации, провести обзор литературы и специальных изданий, составить каталог Интернет-ресурсов;
- представить различные подходы, четко и полно определить рассматриваемые понятия, выявить взаимосвязи понятий и явлений, взаимозависимости и связи с другими вопросами;
- грамотно структурировать материал, ясно, четко и логично его излагать, приводить соответствующие примеры из практики, для иллюстрации положений, тезисов и выводов использовать таблицы, схемы, графики, диаграммы.

Вопросы для самостоятельной подготовки к занятиям практического (семинарского) типа указаны в разделе 4.2.

5.2.1. Учебно-методическое обеспечение самостоятельной работы.

Самостоятельная работа студентом осуществляется для закрепления изученного материала после практических занятий для выполнения домашних заданий, для подготовки к контрольным работам, для изучения дополнительных материалов.

№ п/п	Тип нятия	Указания
Тема 1. Актуальность информационной безопасности в современных условиях		
1	СРС	На основе изучения конспекта лекций и рекомендуемой литературы: 1. определить значение информационной безопасности в ндустриальном обществе; 2. понять основные причины обострения проблемы обеспечения асности информационных технологий; 3. определить информационную безопасность как социальное явление. Рекомендуемая литература: конспект лекций, основная и дополнительная атура
2	СРС	Составить схему «Место информационной безопасности в безопасности рства» Рекомендуемая литература: основная и дополнительная литература
Тема 2. Угрозы и возможные каналы утечки конфиденциальной информации		
3	СРС	Изучить лекционный материал и литературные источники по теме. Дать ы на контрольные вопросы: Какие виды угроз информационной безопасности вы знаете? Что такое конфиденциальная информация? Какие возможные каналы утечки конфиденциальной информации лее уязвимы?
4	СРС	Провести и представить классификацию свойств информации, которые защищать, и угроз информационной безопасности. Конспекты лекций, рекомендованная литература.
Тема 3. Компьютерные вирусы и деструктивные программы		
5	СРС	Разработать классификационную схему видов компьютерных вирусов.
6	СРС	Перечислить известные вредоносные программы типа «троянских ».
7	СРС	Ознакомиться с методами защиты от вредоносных программ и ютерных вирусов. Для подготовки использовать рекомендуемую дополнительную атуру, лекции, интернет ресурсы и иные источники.
8	СРС	Найти информацию по антивирусным программам в сети Интернет. Рекомендованная литература и интернет ресурсы
9	СРС	Подготовить обзор по существующим антивирусным программам. Интернет источники.
Тема 4. Методы защиты информации в автоматизированных системах обработки данных.		
10	СРС	Виды информационных систем. Определение защищенной мационной системы. Классификация методов защиты информации в мационных системах. Использовать конспект лекции и рекомендованную литературу.
11	СРС	Ограничение доступа; разграничение доступа; разделение доступа легий); криптографическое преобразование информации; контроль и учет а; организационные меры; законодательные меры. Использовать конспект лекции и рекомендованную литературу.
Тема 5. Стандарты безопасности компьютерных систем		

№ п/п	Тип нятия	Указания
12	СРС	Необходимость введения стандартов безопасности компьютерных м. Использовать конспект лекции и рекомендованную литературу.
13	СРС	Изучить руководящие документы Гостехкомиссии РФ. Использовать конспект лекции и рекомендованную литературу.
14	СРС	На основании рекомендованных источников составить обзор по ствующим стандартам безопасности автоматизированных систем. Использовать конспект лекции и рекомендованную литературу.
Тема 6. Обеспечение информационной безопасности в Интернет		
15	СРС	Основные источники корпоративных интернет-угроз. Использовать конспект лекции и рекомендованную литературу.
16	СРС	Комплекс взаимодополняющих технических и организационных риятий, защищающих как «размытый» интернетом периметр ративной сети, так и всех конечных пользователей. Использовать конспект лекции и рекомендованную литературу.
17	СРС	Проблемы информационной безопасности в Интернете. Использовать конспект лекции и рекомендованную литературу.
18	СРС	Анализ уязвимости: пассивный и активный Использовать конспект лекции и рекомендованную литературу.
Тема 7. Сеть интранет как основной объект нападений из Интернет		
19	СРС	Основные источники корпоративных интернет-угроз. Криптографическая защита информации. Идентификация и аутентификация. Межсетевые экраны. Использовать конспект лекции и рекомендованную литературу.
		Составить схему методов шифрования.
20	СРС	Комплекс взаимодополняющих технических и организационных риятий, защищающих как «размытый» интернетом периметр ративной сети, так и всех конечных пользователей. Использовать конспект лекции и рекомендованную литературу.
21	СРС	Проблемы информационной безопасности в Интернете. Использовать конспект лекции и рекомендованную литературу.
22	СРС	Анализ уязвимости: пассивный и активный Использовать конспект лекции и рекомендованную литературу.

5.3.Методические рекомендации по подготовке к экзамену по дисциплине

Ответ на экзамене предусматривает устный ответ на теоретические вопросы.

При подготовке к экзамену обучающийся обращается к пройденному материалу, сосредоточенному в конспектах лекций, учебниках и других источниках информации. Повторяя, обобщая, закрепляя и дополняя полученные знания, поднимает их на качественно новый уровень — уровень системы совокупных данных, что позволяет ему понять логику всего предмета в целом. Новые знания обучающийся получает в ходе самостоятельного изучения того, что не было изложено в лекциях и на семинарских занятиях.

Экзамен как особая форма учебного процесса имеет свои особенности, специфические черты и некоторые аспекты, которые необходимо обучающемуся знать и учитывать в своей работе. Это, прежде всего:

• что и как запоминать при подготовке к зачету;

• по каким источникам и как готовиться;

• на чем сосредоточить основное внимание;
• каким образом в максимальной степени использовать программу курса;
• что и как записать, а что выучить дословно и т. п.

На экзамене, как правило, проверяется не столько уровень запоминания обучающимся учебного материала, сколько то, насколько успешно он оперирует теми или иными научными понятиями и категориями, систематизирует факты, как умеет мыслить, аргументировано отстаивать определенную позицию, объясняет и пересказывает заученную информацию.

Программу курса необходимо максимально использовать как в ходе подготовки, так и на самом экзамене. Ведь она включает в себя разделы, темы и основные проблемы, в рамках которых и формируются вопросы для экзамена.

Оптимальным для подготовки к экзамену является вариант, когда обучающийся начинает подготовку к нему с первых занятий по данному курсу.

При подготовке к экзамену по наиболее сложным вопросам, ключевым проблемам и важнейшим понятиям необходимо сделать краткие письменные записи в виде тезисов, планов, определений. Особое внимание в ходе подготовки к экзамену следует уделять конспектам лекций, ибо они обладают рядом преимуществ по сравнению с печатной продукцией. Как правило, они более детальные, что позволяет оценивать современную ситуацию, отражать самую свежую научную и оперативную информацию, отвечать на вопросы, интересующие аудиторию, в данный момент, тогда как при написании и опубликовании печатной продукции проходит определенное время, и материал быстро устаревает, особенно в таких областях знаний, как инфокоммуникационные технологии и информационная безопасность.

В то же время подготовка по одним конспектам лекций недостаточна, необходимо использовать и иную учебную литературу. Не следует бояться дополнительных и уточняющих вопросов на экзамене. Они, как правило, задаются или помимо теоретического вопроса для выявления общей подготовленности, или в рамках билета для уточнения высказанной мысли.

6. Учебная литература и ресурсы информационно-телекоммуникационной сети Интернет, включая перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Основная литература

1. Авдошин, С. М. Технологии и продукты Microsoft в обеспечении информационной безопасности / С. М. Авдошин, А. А. Савельева, В. А. Сердюк. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Вузовское образование, 2017. — 412 c. — ISBN 978-5-4487-0147-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/72341.htm
2. Бондарев В. Введение в информационную безопасность автоматизированных систем. М.: МГТУ им. Н. Э. Баумана, 2016. 252 с.
3. Бабаш А., Баранова Е. Информационная безопасность и защита информации. М.: Инфра-М, 2016. 324 с.
4. Шаньгин В.С. Информационная безопасность компьютерных сетей и систем: учеб. пособие. М.: ИД «Форум» - Инфра-М, 2011. 416 с. Электронный ресурс: http://www.ipa.nw.ru/PAGE/aspirantura/literatura/shangin.pdf.

6.2. Дополнительная литература

1. Бабаш А., Баранова Е., Ларин Д. Информационная безопасность. История защиты информации в России. М.: КДУ, 2015. 736 с.
2. Бирюков А. Информационная безопасность: защита и нападение. 2-е изд. М.: ДМК Пресс, 2017. 474 с. Электронный ресурс: https://vk.com/doc219780081_439946298.
3. Фергюсон Н., Шнайер Б. Практическая криптография. М.: Вильямс, 2017. 420 с.
4. Нестеров С.А. Основы информационной безопасности. М.: Лань, 2016. 324 с.

6.4. Нормативные правовые документы.

1. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.07.2017) «Об информации, информационных технологиях и о защите информации». Статья 16. Защита информации. СПС Консультант.
2. Закон Российской Федерации от 5 марта 1992 г. № 2446-1 «О безопасности». СПС Консультант.
3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных». СПС Консультант.
4. Федеральный закон от 10 января 2002 г. № 1-ФЗ «Об электронной цифровой подписи». СПС Консультант.
5. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». СПС Консультант.
6. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных». СПС Консультант.
7. Постановление Правительства Российской Федерации от 26 июня 1995 г. № 608 «О сертификации средств защиты информации». СПС Консультант.

6.5. Интернет-ресурсы

1. Руководящие документы Гостехкомиссии РФ // www.lghost.ru/lib/security/kurs5/theme06_chapter04.htm
    a. Руководящий документ. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Гостехкомиссия России, 1992.
    b. Руководящий документ. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники. Гостехкомиссия России, 1992.
    c. Руководящий документ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. Гостехкомиссия России, 1992.
    d. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация

автоматизированных систем и требования по защите информации. Гостехкомиссия России, 1992.

e. Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения. Гостехкомиссия России, 1992.

2. SecurituLab. Новости, статьи, блоги компаний // www.securitylab.ru
3. Информационная безопасность. Хаб про информационную безопасность Geektimes // geektimes.ru/hub/infosecurity.
4. Научный журнал «Вопросы кибербезопасности» // cyberrus.com.
5. Журнал “Information Security” // www.itsec.ru/articles2/allpubliks.

6.6. Иные источники.

Не предусмотрены

7.Материально-техническая база, информационные технологии, программное обеспечение и информационные справочные системы

Учебная аудитория для проведения занятий лекционного типа и промежуточной аттестации**.**
Оборудование:
Рабочие места студентов: парты, стулья;
Рабочее место преподавателя: стол, стул;
Доска для рисования маркерами;
Мультимедийный проектор.

Учебная аудитория для проведения практических занятий**.**
Оборудование:
Рабочие места студентов: столы, стулья;
Рабочее место преподавателя: стол, стул;
Доска для рисования маркерами,
Доска интерактивная;
Мультимедийный проектор;
Персональные компьютеры: Core i7 / 8Gb / 2000Gb -15 шт.
Программное обеспечение:
Microsoft Windows 10 Corporate 1909 (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.);
Microsoft Office 2019 (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.);
Google Chrome 76.0.3809.100 (свободная лицензия);
Консультант (контракт с продавцом ЗАО «КонсультантПлюс» от 18.06.2009 № б/н).

Библиотека (абонемент, читальный и компьютерный залы)
Учебная аудитория для самостоятельной работы студента**.**
Оборудование:
Рабочие места студентов: столы, стулья;
Персональные компьютеры.
Программное обеспечение:
Microsoft Windows 10 Corporate 1909 (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.);

Microsoft Office 2019 (контракт с продавцом АО «Ланит» от 18.10.2019 №117/08-19, до 31.12.2020г.);