Министерство науки и высшего образования РФ

ФГБОУ ВО «Уральский государственный лесотехнический университет»

Социально-экономический институт

Кафедра интеллектуальных систем

Рабочая программа дисциплины

включая фонд оценочных средств и методические указания для самостоятельной работы обучающихся

Б1.О.39 Информационная безопасность

Направление подготовки 15.03.04 «Автоматизация технологических процессов и производств»

Направленность (профиль) – «Системы автоматического управления»

Квалификация - бакалавр

Количество зачётных единиц (часов) – 3 (108)

г. Екатеринбург
2023

Разработчик: ст. преподаватель_____/Г.Л. Нохрина/

Рабочая программа утверждена на заседании кафедры интеллектуальных систем (протокол № 6 от «01» февраля 2023 года). .

Зав. кафедрой _____/В. В. Побединский/

Рабочая программа рекомендована к использованию в учебном процессе методической комиссией инженерно-технического института
(протокол № 6 от «2» февраля 2023 года).

Председатель методической комиссии ИТИ _____/А.А. Чижов /

Рабочая программа утверждена директором инженерно-технического института

Директор ИТИ _____/Е.Е. Шишкина/

«3» февраля 2023 года

Оглавление

1. Общие положения. 4
2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы. 4
3. Место дисциплины в структуре образовательной программы 5
4. Объем дисциплины в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 5
5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов 6
5.1 Трудоемкость разделов дисциплины 6
5.2 Содержание занятий лекционного типа 7
5.3 Темы и формы занятий семинарского типа 7
5.4 Детализация самостоятельной работы 8
6. Перечень учебно-методического обеспечения по дисциплине 8
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине 9
7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы 9
7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания 10
7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы 10
7.4 Соответствие шкалы оценок и уровней сформированных компетенций 13
8. Методические указания для самостоятельной работы обучающихся 13
9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине 14
10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине 15

1. Общие положения.

Наименование дисциплины – «Информационная безопасность» относится к дисциплинам (модулям) учебного плана, входящего в состав образовательной программы высшего образования 15.03.04 – Автоматизация технологических процессов и производств (профиль - Системы автоматического управления). Дисциплина «Информационная безопасность» является дисциплиной вариативной части учебного плана.

Нормативно-методической базой для разработки рабочей программы учебной дисциплины «Информационная безопасность» являются:

– Федеральный закон "Об образовании в Российской Федерации", утвержденный приказом Минобрнауки РФ № 273-ФЗ от 29.12.2012;

– Приказ Минобрнауки России № 301 от 05.04.2017 г. Об утверждении порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры.

– Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО) по направлению подготовки 15.03.04 «Автоматизация технологических процессов и производств» (уровень бакалавриата), утвержденный приказом Министерства образования и науки РФ № 730 от 09.08.2021;

– Учебный план образовательной программы высшего образования направления 15.03.04 – Автоматизация технологических процессов и производств (профиль - Системы автоматического управления), подготовки бакалавров по очной, очно-заочной и заочной форме обучения, одобренный Ученым советом УГЛТУ (протокол №3 от 16.03.2023) и утвержденный ректором УГЛТУ (16.03.2023).

Обучение по образовательной программе 15.03.04 – Автоматизация технологических процессов и производств (профиль - Системы автоматического управления) осуществляется на русском языке.

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

Планируемыми результатами обучения по дисциплине, являются знания, умения, владения и/или опыт деятельности, характеризующие этапы/уровни формирования компетенций и обеспечивающие достижение планируемых результатов освоения образовательной программы в целом.

Цель освоения дисциплины – формирование у студентов профессиональных знаний и умений, связанных с использованием методов защиты информации и способов управления качества продукции, процессов, услуг с учетом аспектов информационной безопасности; приобретении студентами актуальных знаний и умений, позволяющих проявить себя в будущей профессиональной деятельности, реализовать свой творческий потенциал путем использования существующего программного обеспечения, а так же поиска новых, более эффективных и функциональных средств защиты информации..

Задачи дисциплины:

- овладение теорией и методологией защиты информации;
- приобретение знаний и умений по организационному обеспечению информационной безопасности и оценке качества процессов и услуг;
- формирование знаний и умений, необходимых для использования нормативно-правовых документов, международных и отечественных стандартов в области информационной безопасности, решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности;
- обретение основ инженерно-технической защиты информации и криптографических методов;
- ознакомление с правовой базой и законодательством Российской Федерации в области информационной безопасности.

Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций**: ОПК-4:** Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности; **ОПК-6:** Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.

В результате изучения дисциплины студент должен:

знать: – теорию информационной безопасности, методологию защиты информации;

– правовое обеспечение информационной безопасности, законодательную базу, систему государственного контроля и управления в области информационной безопасности;

– организационное обеспечение информационной безопасности;

– основные программные средства защиты информации;

– криптографические методы и средства обеспечения информационной безопасности.

уметь: – оценивать состояние организационной защиты информации на объекте;

– определять рациональные меры по обеспечению организационной защите на объекте;

– организовать работу с персоналом с секретной (конфиденциальной) информацией.

владеть: – методами выявления угроз информационной безопасности объекта;

– способами обеспечения режима и секретности на объекте.

3. Место дисциплины в структуре образовательной программы

Данная учебная дисциплина относится к вариативной части учебного плана, что означает формирование в процессе обучения у бакалавра профессиональных знаний и компетенций в рамках выбранного направления, а также навыков производственно-технологической деятельности в подразделениях организаций.

Освоение данной дисциплины является необходимой основой для последующего изучения дисциплин ОПОП и написания выпускной квалификационной работы (см. табл.).

Перечень обеспечивающих, сопутствующих и обеспечиваемых дисциплин

Обеспечивающие	Сопутствующие	Обеспечиваемые
Учебная практика (ознакомительная); Информатика; Основы патентных исследований; Учебная практика (технологическая (проектно-технологическая))	-	Подготовка к процедуре защиты и защита выпускной квалификационной работы

Указанные связи дисциплины «Информационная безопасность» дают обучающемуся системное представление о комплексе изучаемых дисциплин в соответствии с ФГОС ВО, что обеспечивает требуемый теоретический уровень и практическую направленность в системе обучения и будущей деятельности выпускника.

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

Общая трудоемкость дисциплины

Вид учебной работы	Всего академических часов		
	очная форма	**заочная форма**	**очно-заочная форма**
Контактная работа с преподавателем*:	**54,25**	**10,25**	**30,25**
лекции (Л)	22	4	18
практические занятия (ПЗ)	32	6	-
лабораторные работы (ЛР)	-	-	12
промежуточная аттестация (ПА)	0,25	0,25	0,25
Самостоятельная работа обучающихся	**53,75**	**97,75**	**77,75**
изучение теоретического курса	40	70	54
подготовка к текущему контролю знаний	10	24	20
подготовка к промежуточной аттестации	3,75	3,75	3,75
Вид промежуточной аттестации:	**Зачет**	**Зачет**	**Зачет**

Вид учебной работы	Всего академических часов		
	очная форма	**заочная форма**	**очно-заочная форма**
Общая трудоемкость	**3/108**	**3/108**	**3/108**

**Контактная работа обучающихся с преподавателем, в том числе с применением дистанционных образовательных технологий, включает занятия лекционного типа, и (или) занятия семинарского типа, лабораторные занятия, и (или) групповые консультации, и (или) индивидуальную работу обучающегося с преподавателем, а также аттестационные испытания промежуточной аттестации. Контактная работа может включать иные виды учебной деятельности, предусматривающие групповую и индивидуальную работу обучающихся с преподавателем. Часы контактной работы определяются Положением об организации и проведении контактной работы при реализации образовательных программ высшего образования, утвержденным Ученым советом УГЛТУ от 25 февраля 2020 года.*

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов

5.1 Трудоемкость разделов дисциплины

Очная форма обучения

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Основные цели и задачи курса	4	4	-	8	10
2	Угрозы информационной безопасности на предприятии	4	6	-	10	10
3	Основные программные средства защиты информации	6	10	-	16	10
4	Организационное обеспечение информационной безопасности	4	6	-	10	10
5	Правовые аспекты информационной безопасности	4	6	-	10	10
Итого по разделам:		**22**	**32**	**-**	**54**	**50**
Промежуточная аттестация		-	-	-	0,25	3,75
Всего:		**108**				

Очно-заочная форма обучения

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Основные цели и задачи курса	3	-	2	5	10
2	Угрозы информационной безопасности на предприятии	3	-	3	6	16
3	Основные программные средства защиты информации	6	-	3	9	16
4	Организационное обеспечение информационной безопасности	3	-	2	5	16
5	Правовые аспекты информационной безопасности	3	-	2	5	16
Итого по разделам:		**18**	**-**	**12**	**30**	**74**
Промежуточная аттестация		-	-	-	0,25	3,75
Всего:		**108**				

Заочная форма обучения

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
1	Основные цели и задачи курса	0,5	1	-	1,5	10
2	Угрозы информационной безопасности на предприятии	0,5	1	-	1,5	16

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	Всего контактной работы	Самостоятельная работа
3	Основные программные средства защиты информации	2	2	-	4	30
4	Организационное обеспечение информационной безопасности	0,5	1	-	1,5	18
5	Правовые аспекты информационной безопасности	0,5	1	-	1,5	20
Итого по разделам:		**4**	**6**	**-**	**10**	**94**
Промежуточная аттестация		-	-	-	0,25	3,75
Всего:		**108**				

5.2 Содержание занятий лекционного типа

1. Основные цели и задачи курса.

Актуальность информационной безопасности. Основные цели и задачи системы защиты. Источники угроз и атак. Основные классификации атак. Системы критериев оценки защищенности среды.

2. Угрозы информационной безопасности на предприятии

Виды угроз информационной безопасности и их характеристика. Модели нарушителей информационной безопасности на предприятии. Формы преступного посягательства. Оценка ущерба вследствие организационных нарушений информационной безопасности на предприятии.

3. Основные программные средства защиты информации

Программные средства защиты информации. Задачи обеспечения конфиденциальности, целостности и задачи обеспечения наблюдаемости, решаемые программными средствами защиты информации. Изучение основных технологий в области аутентификации данных, криптографии и обеспечении целостности данных. Управление доступом к ресурсам автоматизированной системы.

Технические мероприятия, призванные обеспечить физическую и информационную безопасность. Технические средства для реализации мероприятий данной группы.

Обеспечение безопасности электронного документооборота. Электронная подпись. Методы и средства защиты информации при работе с удаленными базами данных. Стеганография. Компьютерные вирусы и программы типа «Троянский конь». Средства обнаружения и уничтожения компьютерных вирусов.

4. Организационное обеспечение информационной безопасности

Корпоративная политика норм и требований, предъявляемых к сотрудникам на предприятии в отношении защиты корпоративной информации. Подходы к реализации мероприятий по обеспечению информационной безопасности. Построение модели защищенной системы. Обеспечение целостности и конфиденциальности. Примеры реализации политик безопасности информации на различных предприятиях.

5. Правовые аспекты информационной безопасности

Требования к защите информации, изложенные в соответствующих Законах РФ, стандартах и нормативных документах. Сравнение с нормативными документами о защите информации и мер наказания нарушителей законов о защите информации в развитых странах.

5.3 Темы и формы занятий семинарского типа

Учебным планом по дисциплине предусмотрены практические и лабораторные занятия.

№	Наименование раздела дисциплины (модуля)	Форма проведения занятия	Трудоёмкость, час		
			Очная	Заочная	очно-заочная
1	Основные цели и задачи курса	практическая работа	4	1	-
2	Угрозы информационной безопасности на предприятии	практическая работа	6	1	-

№	Наименование раздела дисциплины (модуля)	Форма проведения занятия	Трудоёмкость, час		
			Очная	Заочная	очно-заочная
3	Основные программные средства защиты информации	практическая работа	10	2	-
4	Организационное обеспечение информационной безопасности	практическая работа	6	1	-
5	Правовые аспекты информационной безопасности	практическая работа	6	1	-
6	Основные цели и задачи курса	лабораторная работа	-	-	2
7	Угрозы информационной безопасности на предприятии	лабораторная работа	-	-	3
8	Основные программные средства защиты информации	лабораторная работа	-	-	3
9	Организационное обеспечение информационной безопасности	лабораторная работа	-	-	2
10	Правовые аспекты информационной безопасности	лабораторная работа	-	-	2
Итого:			**32**	**6**	**12**

5.4 Детализация самостоятельной работы

№	Наименование раздела дисциплины (модуля)	Вид самостоятельной работы	Трудоемкость, час		
			очная	заочная	очно-заочная
1	Основные цели и задачи курса	Изучение лекционного материала в соответствии с тематикой	10	10	10
2	Угрозы информационной безопасности на предприятии	Изучение теоретического курса, тестирование	10	16	16
3	Основные программные средства защиты информации	Изучение теоретического курса, тестирование	10	30	16
4	Организационное обеспечение информационной безопасности	Изучение теоретического курса, тестирование	10	18	16
5	Правовые аспекты информационной безопасности	Изучение лекционного материала в соответствии с тематикой	10	20	16
Подготовка к сдаче промежуточной аттестации			3,75	3,75	3,75
Итого:			**53,75**	**97,75**	**77,75**

6. Перечень учебно-методического обеспечения по дисциплине

Основная и дополнительная литература

№	Автор, наименование	Год издания	Примечание
	Основная литература		
1	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : НГТУ, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/152227 .— Режим доступа: для авториз. пользователей..	2019	Полнотекстовый доступ при входе по логину и паролю*

№	Автор, наименование	Год издания	Примечание
2	Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : НГТУ, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/118233. — Режим доступа: для авториз. пользователей.	2018	Полнотекстовый доступ при входе по логину и паролю*
	Дополнительная литература		
3	Информационная безопасность и защита информации : учебное пособие / А. С. Минзов, С. В. Бобылева, П. А. Осипов, А. А. Попов. — Дубна : Государственный университет «Дубна», 2020. — 85 с. — ISBN 978-5-89847-608-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/154490 . — Режим доступа: для авториз. пользователей.	2020	Полнотекстовый доступ при входе по логину и паролю*
4	Защита компьютерной информации : учебное пособие / Е. С. Бондарев, В. М. Васюков, П. Р. Грушевский, О. В. Скулябина. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2019. — 146 с. — ISBN 978-5-907054-82-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157086 . — Режим доступа: для авториз. пользователей.	2019	Полнотекстовый доступ при входе по логину и паролю*

*- *прежде чем пройти по ссылке, необходимо войти в систему.*

Функционирование электронной информационно-образовательной среды обеспечивается соответствующими средствами информационно-коммуникационных технологий.

Электронные библиотечные системы

Каждый обучающийся обеспечен доступом к электронно-библиотечной системе УГЛТУ (http://lib.usfeu.ru/), ЭБС Издательства Лань http://e.lanbook.com/ ЭБС Университетская библиотека онлайн http://biblioclub.ru/, содержащих издания по основным изучаемым дисциплинам и сформированных по согласованию с правообладателями учебной и учебно-методической литературы.

- ЭБС Издательства Лань http://e.lanbook.com/
- ЭБС Университетская библиотека онлайн http://biblioclub.ru
- Электронная база периодических изданий ИВИС https://dlib.eastview.com/
- Электронный архив УГЛТУ(http://lib.usfeu.ru/).

Справочные и информационные системы

1. Справочно-правовая система «Консультант Плюс»
2. Информационно-правовой портал Гарант. Режим доступа: http://www.garant.ru/
3. База данных Scopus компании Elsevier B.V. https://www.scopus.com/
4. Информационная система «ТЕХНОРМАТИВ» - (https://www.technormativ.ru/)
5. «Техэксперт» - профессиональные справочные системы – (http://техэксперт.рус/);

Профессиональные базы данных

1. Научная электронная библиотека elibrary. Режим доступа: http://elibrary.ru/ .
2. Экономический портал (https://institutiones.com/);
3. Информационная система РБК (https://ekb.rbc.ru/;
4. Государственная система правовой информации (http://pravo.gov.ru/;
5. База данных «Единая система конструкторской документации» - (http://eskd.ru/) ;
6. База стандартов и нормативов – (http://www.tehlit.ru/list.htm);

7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Формируемые компетенции	Вид и форма контроля

ОПК-4: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности;	**Промежуточный контроль:** контрольные вопросы зачета **Текущий контроль:** практическая работа в форме тестирования
ОПК-6: Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий.	**Промежуточный контроль:** контрольные вопросы зачета **Текущий контроль:** практическая работа в форме тестирования

7.2 Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Критерии оценивания устного ответа на контрольные вопросы зачета (промежуточный контроль формирования компетенций ОПК-4, ОПК-6):

зачтено – обучающийся для получения зачета должен успешно дать полный, развернутый ответ на поставленный вопрос, продемонстрировать умение работы в электронных системах, показать совокупность осознанных знаний об объекте изучения. Ответ должен быть изложен литературным языком, в логической последовательности, показана способность быстро реагировать на уточняющие вопросы.

не зачтено – студент демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры работы в системе, проявляет отсутствие логичности и последовательности изложения, делает ошибки, которые не может исправить, даже при коррекции преподавателем, отказывается отвечать на занятии.

Критерии оценивания выполнения заданий к практической работе в форме тестирования (текущий контроль формирования компетенций ОПК-4, ОПК-6):

По итогам выполнения тестовых заданий оценка производится по двубальной шкале. При правильных ответах на:

51-100% заданий – оценка *«Зачтено»;*

менее 51% - оценка *«Не зачтено».*

7.3 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Контрольные вопросы к зачету

1. Основные понятия информационной безопасности. Задачи. Объекты защиты информации.
2. Вирусная атака. Классификация вирусов. Антивирусная защита. Виды антивирусных программ.
3. Фильтрация трафика. Обзор персональных программных межсетевых экранов
4. Технология виртуальных частных сетей.
5. Шифрование с несимметричными ключами, обзор.
6. Шифрование с симметричным ключом, обзор.
7. Защита баз данных.
8. Организационные меры по обеспечению безопасности на предприятии.
9. Защита от форс-мажор факторов.
10. Законодательство РФ в области информационной безопасности
11. Средства аутентификации: программные, физические и биологические.
12. Защита информации в операционных системах
13. Электронная цифровая подпись, принципы и примеры использования
14. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
16. Программные средства защиты.
17. Оценка качества безопасности продукции и услуг.
18. Стандарты в области информационной безопасности.

Практическая работа в форме тестирования (текущий контроль)

1. Дополните

_____ - это защищенность информации, информационных ресурсов и систем от случайных или преднамеренных воздействий, которые могут нанести ущерб субъектам информационных отношений

2. Выберите номера правильных ответов

УКАЖИТЕ основные задачи информационной безопасности

1. Обеспечение подлинности и сохранности информации
2. Обеспечение разграничения доступа к информации и ресурсам системы
3. Обеспечение функционирования системы
4. Обеспечение централизованного сбора информации

3. Выберите номер правильного варианта ответа

вид атаки по цели воздействия

1. Активная атака
2. Безусловная атака
3. Атака с обратной связью
4. Атака на нарушение целостности информации

4. Выберите номер правильного варианта ответа

Основная функция брандмауэра

1. Деление сети на подсети
2. Увеличение количества хостов в каждой подключенной подсети
3. Контроль трафика
4. Контроль учетных записей

5. Выберите номер правильного варианта ответа

Определите отличие идентификации от аутентификации

1. Идентификация задает права доступа к объекту, аутентификация – проверку подлинности объекта прав доступа
2. Процедура идентификации описывает объект; аутентификация обеспечивает подлинность объекта
3. Идентификация – успешная попытка представить объект не тем, чем он является; аутентификация – неуспешная попытка
4. Аутентификация – процедура обмена шифрованными ключами для опознания объекта; идентификация – процедура проверки подлинности ключей

6. Выберите номера правильных ответов

к внутренним источникам угроз безопасности относятся

1. Программное обеспечение, в том числе и разработанное на предприятии
2. Каналы связи: Internet, модемная связь, телефонные линии, факс
3. Оборудование, коммуникации, системы водоснабжения
4. Форс-мажор факторы
5. Персонал предприятия, в том числе временные и бывшие работники
6. Всё выше перечисленное

7. Дополните

_____ - это набор факторов, приводящих к сбоям или неработоспособности системы, а также наносящих урон целостности информации

8. Дополните

_____ - это специально написанная программа, способная создавать свои копии и внедрять их в файлы, системные области компьютера, вычислительные с целью выполнения несанкционированных действий на несущем компьютере или сети

9. Выберите номер правильного варианта ответа

определите возможности Пользователя, являющегося членом группы с правом чтения папки и имеющего личное разрешение на запись для той же папки

1. Читать и записывать в эту папку
2. Читать содержимое папки
3. Только входить в папку без возможности получения списка содержимого

4. Осуществлять полный доступ к папке и ее содержимому

10. Выберите номер правильного варианта ответа

укажите меры, необходимые Для защиты от троянских программ

1. Проверять наличие цифровой подписи
2. Никогда не устанавливать на сетевых служебных компьютерах непроверенное программное обеспечение
3. Запрашивать разрешение на прием того или иного активного объекта.
4. Использовать протокол SSL

11. Выберите номер правильного варианта ответа

ШИФРОВАНИЕ, использующее один и тот же ключ как для зашифровки, так и для расшифровки данных, называется

1. Однонаправленным шифрованием
2. Шифрованием на симметричном ключе
3. «Закрытым» шифрованием
4. Шифрованием на ассиметричном ключе

12. Выберите номера правильных ответов

мониторинг трафика включает в себя

1. Проверку интенсивности трафика
2. Фильтрацию трафика
3. Проверку направленности трафика
4. Проверку целостности журналов трафика
5. Проверку содержания трафика
6. Проверку действий пользователя

13. Дополните

_____ подтверждает правильность и подлинность информации о фирме или индивидуальном программисте

14. Выберите номера правильных ответов

В области создания средств защиты информации действуют следующие нормативные акты:

1. Документы ФСБ о информационной безопасности
2. Документы ФАПСИ о разработке и сертификации средств криптографической защиты информации
3. Документы Гостехкомиссии о лицензировании и сертификации деятельности и средств в области защиты информации
4. ГОСТы

15. Выберите номера правильных ответов

По назначению выделяют следующие виды антивирусных программ:

1. Ревизоры
2. Иммунизаторы
3. Резидентные мониторы
4. Цензоры
5. Сканеры

16. Выберите номер правильного варианта ответа

политики паролей не позволяют

1. Задавать минимальную длину пароля
2. Устанавливать алгоритм шифрования пароля
3. Требовать неповторяемости паролей
4. Задавать срок действия пароля

17. Выберите номера правильных ответов

Укажите государственные органы, обеспечивающие информационную безопасность в России

1. Межведомственная комиссия по государственной тайне

2. Федеральное агентство правительственной связи и информации при Президенте РФ
3. Государственная техническая комиссия при президенте РФ
4. Министерство внутренних дел
5. Федеральная служба безопасности
6. Служба внешней разведки

7.4 Соответствие шкалы оценок и уровней сформированных компетенций

Уровень сформированных компетенций	Оценка	Пояснения
Высокий	зачтено	Теоретическое содержание курса освоено полностью, все предусмотренные программой обучения учебные задания выполнены. Обучающийся демонстрирует способность самостоятельного поиска, анализа и синтеза полученной информации. Ориентируется в информационном пространстве и способен использовать информационные системы для решения прикладных задач.
Низкий	не зачтено	Теоретическое содержание курса не освоено, большинство предусмотренных программой обучения учебных заданий либо не выполнены, либо содержат грубые ошибки; дополнительная самостоятельная работа над материалом не привела к какому-либо значительному повышению качества выполнения учебных заданий. Обучающийся не обладает знаниями по имеющимся системам, не способен производить поиск информации, информацию предоставляет не в структурируемом виде.

8. Методические указания для самостоятельной работы обучающихся

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль в контроле за работой студентов).

Самостоятельная работа студентов в вузе является важным видом их учебной и научной деятельности. Самостоятельная работа играет значительную роль в рейтинговой технологии обучения. Поэтому самостоятельная работа должна стать эффективной и целенаправленной работой студентов.

Формы самостоятельной работы студентов разнообразны. Они включают в себя:

- изучение и систематизацию официальных государственных документов: законов, постановлений, указов, нормативно-инструкционных и справочных материалов с использованием информационно-поисковых систем «Консультант Плюс», «Гарант», глобальной сети «Интернет»;
- изучение учебной, научной и методической литературы, материалов периодических изданий с привлечением электронных средств официальной, статистической, периодической и научной информации;
- написание рефератов по теме дисциплины;
- создание презентаций, докладов по выполняемому проекту;
- участие в работе конференций, комплексных научных исследованиях.

В процессе изучения дисциплины «Информационная безопасность» *основными видами самостоятельной работы* являются:

- подготовка к аудиторным занятиям (лекциям и практическим занятиям) и выполнение соответствующих заданий;
- самостоятельная работа над отдельными темами учебной дисциплины в соответствии с учебно-тематическим планом;
- подготовка к зачету.

Самостоятельное выполнение тестовых заданий по всем разделам дисциплины сформированы в фонде оценочных средств (ФОС)

Данные тесты могут использоваться:

– студентами при подготовке к экзамену в форме самопроверки знаний;

– преподавателями для проверки знаний в качестве формы промежуточного контроля на практических занятиях;

– для проверки остаточных знаний студентов, изучивших данный курс.

Тестовые задания рассчитаны на самостоятельную работу без использования вспомогательных материалов. То есть при их выполнении не следует пользоваться учебной и другими видами литературы. Для выполнения тестового задания, прежде всего, следует внимательно прочитать поставленный вопрос. После ознакомления с вопросом следует приступать к прочтению предлагаемых вариантов ответа. Необходимо прочитать все варианты и в качестве ответа следует выбрать индекс (цифровое обозначение), соответствующий правильному ответу. На выполнение теста отводится ограниченное время. Оно может варьироваться в зависимости от уровня тестируемых, сложности и объема теста. Как правило, время выполнения тестового задания определяется из расчета 45-60 секунд на один вопрос. Содержание тестов по дисциплине ориентировано на подготовку студентов по основным вопросам курса. Уровень выполнения теста позволяет преподавателям судить о ходе самостоятельной работы студентов в межсессионный период и о степени их подготовки к экзамену.

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Для успешного овладения дисциплиной используются следующие информационные технологии обучения:

- При проведении лекций используются презентации материала в программе Microsoft Office (PowerPoint), выход на используемые информационные системы и сервисы, профессиональные сайты, использование видеоматериалов различных интернет-ресурсов.
- Практические занятие по дисциплине проводятся с необходимого методического материала (методические указания, справочники, нормативы и т.п.).

На практических занятиях студенты осуществляют работу в электронной информационной среде, электронных-библиотечных системах, профессиональных базах данных и поисковых системах.

В процессе изучения дисциплины учебными целями являются развитие информационной культуры обучающегося, первичное восприятие учебной информации о способах поиска и анализа информации, использование различных систем и сервисов. Посредством использования этих интеллектуальных умений достигаются узнавание ранее усвоенного материала в новых ситуациях, применение абстрактного знания в конкретных ситуациях. Для достижения этих целей используются в основном традиционные информативно-развивающие технологии обучения с учетом различного сочетания пассивных форм (лекция и практическое занятие, консультация, самостоятельная работа) и репродуктивных методов обучения (повествовательное изложение учебной информации, объяснительно-иллюстративное изложение) и практических методов обучения (выполнение заданий).

Университет обеспечен необходимым комплектом лицензионного программного обеспечения:

- семейство коммерческих операционных систем семейства Microsoft Windows;
- офисный пакет приложений Microsoft Office;
- программная система для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ»;
- электронно-библиотечная система «Лань»;
- электронно-библиотечная система «Университетская библиотека онлайн»;
- программное обеспечение виртуализации VM VirtualBox.;
- система электронного обучения на базе LMS Moodle.

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

Реализация учебного процесса осуществляется в специальных учебных аудиториях университета для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Все аудитории укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. При необходимости обучающимся предлагаются наборы демонстрационного оборудования и учебно-наглядных пособий, обеспечивающие тематические иллюстрации. Самостоятельная работа обучающихся выполняется в специализированной аудитории, которая оборудована учебной мебелью, компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УГЛТУ.

Есть помещение для хранения и профилактического обслуживания учебного оборудования.

Требования к аудиториям

Наименование специальных помещений и помещений для самостоятельной работы	**Оснащенность специальных помещений и помещений для самостоятельной работы**
Помещение для лекционных занятий, групповых и индивидуальных консультаций, текущей и промежуточной аттестации.	Переносная мультимедийная установка (проектор, экран). Учебная мебель
Помещение для лабораторных и практических занятий и промежуточной аттестации и самостоятельной работы	Столы компьютерные, стулья. Персональные компьютеры. Выход в Интернет, в электронную информационно-образовательную среду УГЛТУ.
Помещение для хранения и профилактического обслуживания учебного оборудования	Стеллажи. Раздаточный материал.