

	ЧОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2022	
	Информационная безопасность	Взамен РПД-2015	Стр. 1 из 24

ОДОБРЕНО
Учебно-методическим советом
Протокол № 1
«2» сентября 2022 г.

УТВЕРЖДАЮ
Ректор
_____ В.Ю. Филоненко
«2» сентября 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность

(наименование дисциплины)

Направление подготовки: 38.03.05 – Бизнес- информатика

Профиль подготовки: Электронный бизнес

Квалификация выпускника: бакалавр

Форма обучения: очная/очно-заочная

Кафедра прикладной информатики в экономике

Рассмотрено и одобрено на заседании кафедры

«1» сентября 2022 г. Протокол № 1

Зав. кафедрой: канд. техн. наук Лаврухина Т.В.

Липецк –2022 г.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 2 из 24

СОДЕРЖАНИЕ

1. Цели освоения дисциплины	3
2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП	3
2. Место дисциплины в структуре ОП ВО	4
4. Объем дисциплины (модуля) в зачетных единицах с указанием академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся.....	4
5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических или астрономических часов и видов учебных занятий	4
6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)	10
7. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).....	11
8. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)	17
а) Основная учебная литература	17
б) Дополнительная учебная литература:	17
9. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины (модуля)	18
10. Методические указания для обучающихся по освоению дисциплины (модуля)	18
11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем	21
12. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)	22
Лист согласования	23
Лист регистрации изменений	24

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 3 из 24

1. Цели освоения дисциплины

Целями изучения дисциплины «Информационная безопасность» являются ознакомление студентов с современными способами и средствами защиты информации, реализуемыми в виде технических, программных средств или организационных мер, экономическими и правовыми принципами их функционирования, а также возможностями использования защиты в работе с информационными ресурсами в различных областях экономики и бизнеса.

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

В процессе освоения тематики дисциплины у студента формируются следующие компетенции:

способностью решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-1);

выбор рациональных информационных систем и информационно-коммуникативных технологий решения для управления бизнесом (ПК-3).

В результате освоения дисциплины обучающийся должен:

знать:

- принципы информационной безопасности;
- основные угрозы информационной безопасности;
- структуру коммерческой тайны предприятия;
- отличия между коммерческой тайной и интеллектуальной собственностью предприятия;
- методы и критерии оценки эффективности мероприятий по защите информации.

уметь:

- различать правовые, организационные и технические мероприятия по защите информации;
- выявлять и классифицировать угрозы информационной безопасности предприятия;
- планировать мероприятия по защите информации, исходя из известных угроз и финансовых возможностей предприятия;
- рассчитывать эффективность мероприятий по защите информации.

владеть:

- навыками работы в сети Интернет;
- средствами борьбы с компьютерными вирусами;
- механизмами организации раздельного доступа к файлам и папкам на компьютере.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 4 из 24

2. Место дисциплины в структуре ОП ВО

Дисциплина «Информационная безопасность» входит в базовую часть блока Б.1 направления (Б.1.Б.36). Читается в 1 семестре – очная форма обучения, уст., 9 семестре – заочная форма обучения, базируется на знаниях, полученных в средней общеобразовательной школе по предмету «Информатика» и тесно связана с изучением тематики дисциплины «Право», является основой для последующего изучения дисциплин направления: «Проектирование систем интернет-коммерции».

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

Объем дисциплины - 2 зачетных единицы, 72 часа.

Очная форма обучения: контактная работа – 36 час. (лекции – 18 час.; лабораторные занятия - 18 час.); самостоятельная работа обучающихся – 36 часов.

Заочная форма обучения: контактная работа - 8 часов (лекции – 4 час.; консультации – 4 час.); самостоятельная работа обучающихся – 64 часа.

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

№ п/п	Раздел дисциплины	Семестр	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах) очная/заочная форма обучения				Формы текущего контроля успеваемости Форма промежуточной аттестации
			лекции	лабор. занятия/конс.	Интерактивные формы занятий	СРС	
1	Информационные технологии в экономике и управлении. Экономическая эффективность информационных технологий		2/0,5	2/0,5		2/6	Собеседование
2	Структура информационных ресурсов предприятия. Понятие интеллектуальной собственности и коммерческой тайны		2/0,5	2/0,5		4/6	Блиц-опрос.
3	Угрозы информационной безопасности предприятия. Классификация средств		4/0,5	4/0,5	Групповая игра «Защита предприятия»	2/6	Оценивание работы в игре

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 5 из 24

	защиты информации						
4	Правовые средства защиты информации от несанкционированного доступа		2/0,5	2/0,5	Конкурс по составлению документов в малых группах	2/6	Подведение итогов конкурса
5	Организационные средства защиты информации от несанкционированного доступа.		2/0,5	2/0,5		4/7	Опрос
6	Технические средства защиты информации от несанкционированного доступа		2/0,5	2/0,5		4/7	Опрос
7	Защита информации от повреждения		2/0,5	2/0,5	Рассмотрение ситуаций и обсуждения в малых группах	4/7	Оценивание работы в группах
8	Экономическая эффективность мероприятий по защите информации		2/0,5	2/0,5	Рассмотрение ситуаций и обсуждения в малых группах	2/7	Оценивание работы в группах
						12/12	Подготовка ПР, зачет
	Итого: 1,2 семестры		18/4	18/4		36/64	Зачет

Распределение компетенций по темам дисциплины

№ п/п	Раздел дисциплины	Осваиваемые компетенции
1	Информационные технологии в экономике и управлении. Экономическая эффективность информационных технологий	ОПК-1
2	Структура информационных ресурсов предприятия. Понятие интеллектуальной собственности и коммерческой тайны	ОПК-1
3	Угрозы информационной безопасности предприятия. Классификация средств защиты информации	ОПК-1 ПК-3
4	Правовые средства защиты информации от несанкционированного доступа	ОПК-1
5	Организационные средства защиты информации от несанкционированного доступа.	ОПК-1 ПК-3
6	Технические средства защиты информации от несанкционированного доступа	ОПК-1 ПК-3,
7	Защита информации от повреждения	ОПК-1 ПК-3
8	Экономическая эффективность мероприятий по защите информации	ОПК-1 ПК-3

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 6 из 24

Методические указания для преподавателей

Рекомендуемые средства, методы обучения, способы учебной деятельности, применение которых для освоения конкретных модулей рабочей учебной программы наиболее эффективно:

- обучение теоретическому материалу рекомендуется основывать на основной и дополнительной литературе, рекомендуется в начале семестра ознакомить студентов с программой дисциплины, перечнем теоретических вопросов для текущего промежуточного и итогового контроля знаний, что ориентирует и поощрит студентов к активной самостоятельной работе;

- рекомендуется проводить лекционные занятия с использованием мультимедийной техники (проектора). На первом занятии до студентов должны быть доведены требования по освоению материала, правила написания и сдачи лабораторной работы и ИЗ, перечень рекомендуемой литературы. Желательно провести обзор тем, которые будут изучены в течение семестра с тем, чтобы студенты более осознанно подходили к выполнению работ. Также часть занятий проводятся в активной и интерактивной форме (в соответствии с ПО 07.08-13-2013 Интерактивное обучение);

- консультации выполняются как в индивидуальном порядке, так и в малых группах, в форме лабораторных или практических занятий. При выполнении работы задание выдается как преподавателем, так и с учетом возможности выбора самого студента (при условии обязательного согласования с преподавателем этого выбора), работа в малых группах.

Предусматривается защита лабораторных работ с обсуждением в группе. При этом оценивается активность участия в групповом обсуждении, конструктивность и обоснованность замечаний по выполненной работе.

Учебный процесс, опирающийся на использование интерактивных методов обучения, организуется с учетом включенности в процесс познания всех студентов группы без исключения. Совместная деятельность означает, что каждый вносит свой особый индивидуальный вклад, в ходе работы идет обмен знаниями, идеями, способами деятельности. Организуются индивидуальная, парная и групповая работа, используется проектная работа, ролевые игры, осуществляется работа с документами и различными источниками информации и т.д.

Интерактивные методы основаны на принципах взаимодействия, активности обучаемых, опоре на групповой опыт, обязательной обратной связи. Создается среда образовательного общения, которая характеризуется открытостью, взаимодействием участников, равенством их аргументов, накоплением совместного знания, возможностью взаимной оценки и контроля.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 7 из 24

Лекционные занятия

Тема 1. Информационные технологии в экономике и управлении. Экономическая эффективность информационных технологий

Цели и задачи дисциплины. Понятие информационной технологии и ее структура. Автоматические и автоматизированные информационные технологии. Автоматические информационные технологии в производстве. Информационные технологии маркетинга: Интернет-реклама, электронная коммерция, маркетинговые исследования в Интернет. Информационные технологии управления материальными ресурсами. Внедрение информационных технологий как инвестиционный проект. Измерение экономического эффекта от информационной технологии.

Тема 2. Структура информационных ресурсов предприятия. Понятие интеллектуальной собственности и коммерческой тайны

Понятие об информационных ресурсах предприятия. Понятия интеллектуальной собственности и коммерческой тайны, их структура. Принципы информационной безопасности.

Тема 3. Угрозы информационной безопасности предприятия. Классификация средств защиты информации

Угрозы информационным ресурсам предприятия: угрозы несанкционированного доступа и угрозы повреждения информации; угрозы криминогенного характера, природного и техногенного характера, угрозы, связанные с неквалифицированным использованием информационными ресурсами. Промышленный шпионаж, его цели и методы. Внутренние и внешние факторы, способствующие промышленному шпионажу. Характеристика каналов утечки информации. Активный и пассивный доступ к информационным ресурсам.

Тема 4. Правовые средства защиты информации от несанкционированного доступа

Понятие о правовых средствах защиты информации. Законы, регулирующие деятельность по защите информации: патентный закон, антимонопольное законодательство, закон об информации. Их основные положения. Охрана объектов интеллектуальной собственности. Патентование и лицензирование. Проблемы, возникающие при реализации правовых мер защиты информации.

Тема 5. Организационные средства защиты информации от несанкционированного доступа

Организационные меры защиты информации: при проведении деловых переговоров, при работе с ЭВМ, при работе с документами, при работе с персоналом. Специализированный отдел по борьбе с промышленным шпионажем: плюсы и минусы. Организационные меры охраны конфиденциальных сведений на предприятиях малого бизнеса.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 8 из 24

Тема 6. Технические средства защиты информации от несанкционированного доступа

Технические средства противодействия промышленному шпионажу. Защита ЭВМ и электронных носителей информации. Защита документации. Защита каналов связи. Защита программ и электронных баз данных. Основные положения криптографии. Характеристики криптоалгоритмов.

Тема 7. Защита информации от повреждения

Направления защиты информации от повреждения: защита компьютерной техники и электронных носителей информации, защита информации при передаче по каналам связи, защита от неквалифицированного пользователя. Организационные и технические средства защиты информации от повреждения. Дублирование важной информации на разнотипных носителях. Ограничение доступа. Технические средства защиты информации от повреждения. Пароли и системы с многоуровневым доступом. Антивирусные программы. Повреждение информации в каналах связи и средства борьбы с ним.

Тема 8. Экономическая эффективность мероприятий по защите информации

Частный функциональный критерий информационной безопасности (ЧФК ИБ). Формула ЧФК ИБ для мероприятий по предотвращению несанкционированного доступа. Структура понесенного и предотвращенного ущерба от несанкционированного доступа к информации. Формула ЧФК ИБ для мероприятий по обеспечению сохранности массивов информации. Структура понесенного и предотвращенного ущерба в этом случае. Структура затрат на защиту информации.

Темы лабораторных занятий, консультаций

Тема 1. Информационные технологии в экономике и управлении

Автоматические и автоматизированные информационные технологии.

Автоматические информационные технологии в производстве.

Информационные технологии маркетинга: Интернет-реклама, электронная коммерция, маркетинговые исследования в Интернет.

Тема 2. Структура информационных ресурсов предприятия

Построение структурированной информационной системы предприятия с соблюдением принципов информационной безопасности.

Форма (ОАО, ООО, ИП, интернет-магазин и т.п.) и отрасль (сфера деятельности) предприятия – задается преподавателем или предполагается выбор студента.

Тема 3. Угрозы информационной безопасности предприятия. Классификация средств защиты информации

Методы противодействия промышленному шпионажу. Ознакомление с внутренними и внешними факторами, способствующими промышленному шпионажу. Изучение каналов утечки информации. Активный и пассивный доступ к информационным ресурсам.



Тема 4. Правовые средства защиты информации от несанкционированного доступа

Работа с нормативно-правовой базой информационно-поисковой информационной системой «Гарант», «Консультант плюс». Практическая работа с законами, регулирующими деятельность по защите информации: патентный закон, антимонопольное законодательство, закон об информации. Их основные положения. Охрана объектов интеллектуальной собственности. Патентование и лицензирование. Проблемы, возникающие при реализации правовых мер защиты информации.

Тема 5. Организационные средства защиты информации от несанкционированного доступа

Ознакомление с организационными мерами защиты информации: при проведении деловых переговоров, при работе с ЭВМ, при работе с документами, при работе с персоналом. Ознакомление с организационными мерами охраны конфиденциальных сведений на предприятиях малого бизнеса.

Тема 6. Технические средства защиты информации от несанкционированного доступа

Технические средства противодействия промышленному шпионажу. Защита ЭВМ и электронных носителей информации. Защита документации. Защита каналов связи. Защита программ и электронных баз данных. Основные положения криптографии. Характеристики криптоалгоритмов.

Тема 7. Защита информации от повреждения

Направления защиты информации от повреждения: защита компьютерной техники и электронных носителей информации, защита информации при передаче по каналам связи, защита от неквалифицированного пользователя. Технические средства защиты информации от повреждения. Дублирование важной информации на разнотипных носителях. Ограничение доступа. Технические средства защиты информации от повреждения. Пароли и системы с многоуровневым доступом. Антивирусные программы. Повреждение информации в каналах связи и средства борьбы с ним.

Тема 8. Экономическая эффективность мероприятий по защите информации

Частный функциональный критерий информационной безопасности (ЧФК ИБ). Формула ЧФК ИБ для мероприятий по предотвращению несанкционированного доступа. Структура понесенного и предотвращенного ущерба от несанкционированного доступа к информации. Формула ЧФК ИБ для мероприятий по обеспечению сохранности массивов информации. Структура понесенного и предотвращенного ущерба в этом случае. Структура затрат на защиту информации.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 10 из 24

6. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Рекомендуемый режим и характер различных видов учебной, в том числе самостоятельной, работы:

– изучение теоретического материала определяется рабочей учебной программой дисциплины, включенными в нее календарным планом изучения дисциплины и перечнем литературы, конспектом лекций (электронным – при его наличии); настоятельно рекомендуется при подготовке к очередной лекции освежить в памяти, по указанию лектора, материал предшествующих дисциплин рабочего учебного плана, на который опирается изучаемый раздел данной дисциплины;

– ПР / ИЗ выполняются в соответствии с изданными типографским или электронным способом методическими указаниями, регламентирующими все этапы выполнения и сдачи работ, определяют свой вклад в рейтинговую оценку;

Планирование времени на самостоятельную работу, необходимого на изучение настоящей дисциплины, лучше всего осуществлять на весь семестр (в соответствии с ПО 07.08-12-2013 Организация самостоятельной работы студентов), предусматривая при этом регулярное повторение пройденного материала. Материал, законспектированный на лекциях, необходимо регулярно дополнять сведениями из литературных источников, представленных в списке рекомендуемой литературы. По каждой из тем для самостоятельного изучения, приведенных в программе дисциплины, следует сначала прочитать рекомендованную литературу и при необходимости составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме и нужных для освоения последующих разделов.

Для расширения знаний по дисциплине рекомендуется использовать Интернет-ресурсы: проводить поиск в различных поисковых системах, таких как www.rambler.ru, www.yandex.ru, www.google.ru, www.yahoo.ru и использовать материалы сайтов, рекомендованных преподавателем на лекционных занятиях.

При подготовке к зачету следует руководствоваться перечнем вопросов для подготовки к итоговому контролю. При этом, прежде всего, следует уяснить суть основных понятий дисциплины, проработать учебные материалы основной и дополнительной литературы, а также литературы из электронно-библиотечной системы, рекомендованных для изучения дисциплины.

Распределение времени на самостоятельную работу студента

№ п/п	Вид самостоятельной работы	Количество времени (часы) очная/заочная форма обучения
1	Проработка материала лекций, учебных материалов. Самостоятельная проработка тем	10/18
2	Подготовка к консультациям. Самостоятельная проработка тем	14/34
3	Подготовка к выполнению ПР	4/4
4	Подготовка к зачету	8/8
	Итого	36/64

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 11 из 24

Вопросы для самостоятельной работы студентов

1. Понятие информационной технологии.
2. Структура информационной технологии.
3. Классификация информационных технологий.
4. АСУТП, структура и алгоритм работы.
5. АСУП, структура и алгоритм работы.
6. Информационные технологии планирования и контроля.
7. Экономическая эффективность внедрения информационных технологий.
8. Понятие интеллектуальной собственности и коммерческой тайны.
9. Структура коммерческой тайны предприятия.
10. Классификация угроз информационной безопасности предприятия.
11. Угрозы коммерческой тайне предприятия.
12. Угрозы сохранности информации.
13. Цели промышленного шпионажа.
14. Средства промышленного шпионажа.
15. Характеристика каналов утечки информации.
16. Принципы информационной безопасности предприятия.
17. Классификация средств и мероприятий по защите информации от несанкционированного доступа.
18. Законодательные акты, регулирующие защиту информации.
19. Недостатки правовой защиты.
20. Организационные мероприятия по защите информации.
21. Защита информации при проведении деловых переговоров.
22. Технические средства защиты информации, хранящейся в электронном виде.

Образовательные технологии

При реализации программы дисциплины используются различные образовательные технологии: во время аудиторных занятий занятия проводятся в виде

- лекций с использованием ПК и компьютерного проектора;
- занятий в компьютерном классе с обсуждением в группе.

Наряду с традиционными преподавательскими методиками изучение данной дисциплины предполагает реализацию следующих интерактивных учебных методов:

- метод дискуссии;
- метод конкретных ситуаций;
- метод обучения действием.

Предполагается возможность внеаудиторных он-лайн коммуникаций преподавателя со студентами, а также распространения необходимых материалов и осуществления контроля посредством использования возможностей Интернета.

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

Примерный перечень вопросов для подготовки к зачету

1. Понятие информационной технологии. Структура информационной технологии.
2. Классификация информационных технологий.
3. АСУТП. Структура и алгоритм работы.



4. АСУП. Структура и алгоритм работы.
5. Информационные технологии планирования и контроля.
6. Экономическая эффективность внедрения информационных технологий.
7. Понятие интеллектуальной собственности и коммерческой тайны.
8. Структура коммерческой тайны предприятия.
9. Классификация угроз информационной безопасности предприятия.
10. Угрозы коммерческой тайне предприятия.
11. Угрозы сохранности информации.
12. Цели промышленного шпионажа.
13. Средства промышленного шпионажа.
14. Характеристика каналов утечки информации.
15. Принципы информационной безопасности предприятия.
16. Классификация средств и мероприятий по защите информации от несанкционированного доступа.
17. Законодательные акты, регулирующие защиту информации. Недостатки правовой защиты.
18. Организационные мероприятия по защите информации.
19. Защита информации при проведении деловых переговоров.
20. Технические средства защиты информации, хранящейся в электронном виде.
21. Технические средства защиты информации на бумажных носителях.
22. Технические средства защиты информации в процессе ее передачи по каналам связи.
23. Организационные мероприятия по защите информации от повреждения.
24. Технические средства защиты информации от повреждения и их классификация.
25. Экономическая эффективность мер по борьбе с несанкционированным доступом к информации.
26. Экономическая эффективность мер по защите информации от повреждения.

Текущий контроль успеваемости по дисциплине может учитывать следующее:

- выполнение студентом всех видов работ, предусмотренных программой дисциплины (в том числе ответы на семинарах, коллоквиумах, при тестировании; подготовка докладов и рефератов; выполнение лабораторных и проверочных работ, индивидуальных заданий, участие в деловых играх и т.п.);

- посещаемость;

- самостоятельная работа студента;

- исследовательская работа и т.д.

Оценка должна носить комплексный характер и учитывать достижения студента по основным компонентам учебного процесса.

Оценка знаний по 100-балльной шкале в соответствии с критериями института реализуется следующим образом:

- менее 53 балла – «неудовлетворительно»;
- от 53 до 79 баллов – «удовлетворительно»;
- от 80 до 92 баллов – «хорошо»;
- 93 балла и выше – «отлично».

Критерии оценок промежуточной аттестации

Оценка за работу в течение семестра складывается из результатов текущего контроля знаний и работы в течение семестра.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 13 из 24

Текущий контроль

№ п/п	Форма текущего контроля	Баллы
1.	Выполнение студентом всех видов работ, предусмотренных программой дисциплины (в том числе ответы на семинарах, коллоквиумах, при тестировании; подготовка докладов и рефератов; выполнение лабораторных и проверочных работ, индивидуальных заданий, участие в деловых играх и т.п.)	45
2.	Подготовка ПР	15

Итого: текущий контроль знаний – 60 баллов.

Оценка за работу в семестре:

1. Присутствие и работа на лекции (конспект) – 1 балл;
2. Присутствие на консультации – 1 балл;
3. Ответы на занятиях – 2 балла;
4. Активность на занятиях – 1 балл;
5. Самостоятельная работа (выполнение домашнего творческого задания, участие в занятиях в интерактивной форме) – 15 баллов;
6. Контрольный опрос – 5 баллов;

Итого: оценка за работу в семестре – 40 баллов.

Результаты текущего контроля успеваемости оцениваются по 100-балльной системе. Аттестованным считается студент, набравший 53 балла и выше.

Промежуточная аттестация - в форме зачета, который проводится в устной форме в виде ответов на вопросы билета.

При этом оценка знаний студентов осуществляется в баллах в комплексной форме с учетом:

- оценки по итогам текущего контроля знаний;
- оценки промежуточной аттестации в ходе зачета.

Содержание билета:

- 1-е задание – 50 баллов;
- 2-е задание – 50 баллов;

Итого: за промежуточную аттестацию (результат в ходе зачета) – 100 баллов.

Тематика ПР /индивидуальных заданий

1. Угрозы сохранности информации.
2. Цели промышленного шпионажа.
3. Средства промышленного шпионажа.
4. Характеристика каналов утечки информации.
5. Принципы информационной безопасности предприятия.
6. Классификация средств и мероприятий по защите информации от несанкционированного доступа.
7. Законодательные акты, регулирующие защиту информации. Недостатки правовой защиты.
8. Организационные мероприятия по защите информации.
9. Защита информации при проведении деловых переговоров.
10. Технические средства защиты информации, хранящейся в электронном виде.
11. Технические средства защиты информации на бумажных носителях.
12. Технические средства защиты информации в процессе ее передачи по каналам.
13. Организационные мероприятия по защите информации от повреждения.
14. Технические средства защиты информации от повреждения и их классификация.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 14 из 24

15. Экономическая эффективность мер по борьбе с несанкционированным доступом к информации.
16. Экономическая эффективность мер по защите информации от повреждения.

Примерные тесты для промежуточного контроля

1. *Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это....*

1. **информационная война**
2. информационное оружие
3. информационное превосходство

2. *Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.*

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. **конфиденциальная информация**

3. *Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена*

1. **конфиденциальность**
2. целостность
3. доступность
4. аутентичность
5. апеллеруемость

4. *Гарантия того, что АС ведет себя в нормальном и внештатном режиме так, как запланировано*

1. **надежность**
2. точность
3. контролируемость
4. устойчивость
5. доступность

5. *Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.*

1. принцип системности
2. принцип комплексности
3. принцип непрерывной защиты
4. принцип разумной достаточности
5. **принцип гибкости системы**

6. *В классификацию вирусов по способу заражения входят*

1. опасные



2. файловые
 3. **резидентные**
 4. загрузочные
 5. файлово -загрузочные
 6. **нерезидентные**
7. *Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это...*
1. **комплексное обеспечение ИБ**
 2. безопасность АС
 3. угроза ИБ
 4. атака на АС
 5. политика безопасности
8. *Вирусы, не связывающие свои копии с файлами, а создающие свои копии на дисках, не изменяя других файлов, называются:*
1. компаньон - вирусами
 2. **черви**
 3. паразитические
 4. студенческие
 5. призраки
 6. стелс - вирусы
 7. макровирусы
9. *К видам системы обнаружения атак относятся :*
1. системы, обнаружения атаки на ОС
 2. системы, обнаружения атаки на конкретные приложения
 3. системы, обнаружения атаки на удаленных БД
 4. **все варианты верны**
10. *Автоматизированная система должна обеспечивать*
1. надежность
 2. **доступность**
 3. **целостность**
 4. контролируемость
11. *Основными компонентами парольной системы являются*
1. **интерфейс администратора**
 2. хранимая копия пароля
 3. **база данных учетных записей**
 4. все варианты верны
12. *Некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации это*
1. идентификатор пользователя
 2. **пароль пользователя**
 3. учетная запись пользователя
 4. парольная система



13. К принципам информационной безопасности относятся

1. скрытость
2. масштабность
3. **системность**
4. **законность**
5. **открытости алгоритмов**

14. К вирусам, изменяющим среду обитания, относятся:

1. черви
2. студенческие
3. **полиморфные**
4. спутники

15. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это...

1. **Защита информации**
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

16. Система физической безопасности включает в себя следующие подсистемы:

1. **оценка обстановки**
2. скрытность
3. **строительные препятствия**
4. **аварийная и пожарная сигнализация**

17. Какие степени сложности устройства Вам известны

1. упрощенные
2. **простые**
3. **сложные**
4. оптические
5. встроенные

18. К механическим системам защиты относятся:

1. **проволака**
2. **стена**
3. сигнализация
4. **вы**

19. Какие компоненты входят в комплекс защиты охраняемых объектов:

1. **сигнализация**
2. **охрана**
3. **датчики**
4. **телевизионная система**

20. К выполняемой функции защиты относится:

1. внешняя защита
2. внутренняя защита
3. **все варианты верны**

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 17 из 24

21. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. **Компьютерная безопасность**
3. Защищенность информации
4. Безопасность данных

22. Средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрепятствования доступа к ним это:

1. информационная война
2. **информационное оружие**
3. информационное превосходство

23. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:

1. государственная тайна
2. **коммерческая тайна**
3. банковская тайна
4. конфиденциальная информация

24. Гарантия того, что при хранении или передаче информации не было произведено несанкционированных изменений:

1. конфиденциальность
2. **целостность**
3. доступность
4. аутентичность
5. апеллируемость

25. Гарантия точного и полного выполнения команд в АС:

1. надежность
2. **точность**
3. контролируемость
4. устойчивость
5. доступность

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

8.1. Основная учебная литература

1. [Теория информационной безопасности и методология защиты информации: учебное пособие Загинайлов Ю. Н.](#) Директ-Медиа • 2015 год • 253 страницы

8.2. Дополнительная учебная литература:

1. Ярочкин В.И. Информационная безопасность: учебник. – 5-е изд., испр. – М.: Академический проект, 2008. – 544 с. (гриф)
2. Келина А.Ю. Основы информационной безопасности: учебное пособие. – Липецк: ЛЭГИ, 2005. – 40с.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 18 из 24

В соответствии с договором студентам и преподавателям института предоставляется право доступа к электронному периодическому изданию Электронно-библиотечной системы «КнигаФонд» (www.knigafund.ru).

Книги, рекомендуемые для занятий по дисциплине, доступные в электронном периодическом издании:

1. [Безопасность информационных систем: курс Кияев В., Граничин О.](#) Национальный Открытый Университет «ИНТУИТ» • 2016 год • 192 страницы
2. [Основы информационной безопасности : курс визуальных лекций: учебное пособие Загинайлов Ю. Н.](#) Директ-Медиа • 2015 год • 105 страниц
3. Аверченков В.И., Рытов М.Ю. Организационная защита информации: учебное пособие для вузов. - М.: ФЛИНТА, 2011. - 184 с. / <http://www.knigafund.ru/books/116220>
4. Защита персональных данных в организациях: монография [Аверченков В.И., Рытов М.Ю., Гайнулин Т.Р.](#) ФЛИНТА 2011 г. 124 с. <http://www.knigafund.ru/books/175011>
5. Служба защиты информации: организация и управление: учебное пособие для вузов [Аверченков В.И., Рытов М.Ю.](#) ФЛИНТА 2011 г. 186 с.
6. [Информационная безопасность: учебно-практическое пособие Башлы П.Н., Баранова Е. К., Бабаш А. В.](#) Евразийский открытый институт • 2011 год • 375 страниц
7. [Аудит информационной безопасности органов исполнительной власти: учебное пособие](#) Флинта • 2011 год • 100 страниц <http://www.knigafund.ru/books/116368>

9. Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины (модуля)

1. Портал «Открытые системы»: <http://www.osp.ru>
2. Информационный портал, оперативно и ежедневно рассказывающий о событиях в области защиты информации, интернет права и новых технологиях <http://www.securitylab.ru/>
3. Проект Искусство управления информационной безопасностью. Интернет порталы, посвященные вопросам информационной безопасности <http://www.iso27000.ru/katalog-sylok/informacionnye-portaly>

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

Планирование и организация времени, необходимого для изучения дисциплины

Важным условием успешного освоения дисциплины является создание системы правильной организации труда, позволяющей распределить учебную нагрузку равномерно в соответствии с графиком образовательного процесса. Большую помощь в этом может оказать составление плана работы на семестр, месяц, неделю, день. Его наличие позволит подчинить свободное время целям учебы, трудиться более успешно и эффективно. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подвести итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине они произошли. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана. Все задания к практическим занятиям, а также задания, вынесенные на самостоятельную работу, рекомендуется выполнять непосредственно после соответствующей темы лекционного курса, что способствует лучшему усвоению материала, позволяет своевременно выявить и устранить «про-

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 19 из 24

белы» в знаниях, систематизировать ранее пройденный материал, на его основе приступить к овладению новыми знаниями и навыками.

Система обучения основывается на рациональном сочетании нескольких видов учебных занятий (в первую очередь, лекций и практических занятий), работа на которых обладает определенной спецификой.

Подготовка к лекциям

Знакомство с дисциплиной происходит уже на первой лекции, где от студента требуется не просто внимание, но и самостоятельное оформление конспекта. При работе с конспектом лекций необходимо учитывать тот фактор, что одни лекции дают ответы на конкретные вопросы темы, другие – лишь выявляют взаимосвязи между явлениями, помогая студенту понять глубинные процессы развития изучаемого предмета как в истории, так и в настоящее время.

Конспектирование лекций – сложный вид вузовской аудиторной работы, предполагающий интенсивную умственную деятельность студента. Конспект является полезным тогда, когда записано самое существенное и сделано это самим обучающимся. Не надо стремиться записать дословно всю лекцию. Такое «конспектирование» приносит больше вреда, чем пользы. Целесообразно вначале понять основную мысль, излагаемую лектором, а затем записать ее. Желательно запись осуществлять на одной странице листа или оставляя поля, на которых позднее, при самостоятельной работе с конспектом, можно сделать дополнительные записи, отметить непонятные места.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большей степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает лектор, отмечая наиболее важные моменты в лекционном материале замечаниями «важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, всегда необходимо использовать не только учебник, но и ту литературу, которую дополнительно рекомендовал лектор. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Подготовка к практическим / лабораторным занятиям

Подготовку к каждому практическому занятию студент должен начать с ознакомления с планом практического занятия, который отражает содержание предложенной темы. Тщательное продумывание и изучение вопросов плана основывается на проработке текущего материала лекции, а затем изучения обязательной и дополнительной литературы, рекомендованной к данной теме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы практикума, его выступлении и участии в коллективном обсуждении вопросов изучаемой темы, правильном выполнении практических заданий и контрольных работ.

В процессе подготовки к практическим занятиям, студентам необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей



полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов свое отношение к конкретной проблеме.

Рекомендации по написанию практических (проверочных) работ / индивидуальных заданий

Рекомендации по работе с литературой

Работу с литературой целесообразно начать с изучения общих работ по теме, а также учебников и учебных пособий. Далее рекомендуется перейти к анализу монографий и статей, рассматривающих отдельные аспекты проблем, изучаемых в рамках курса, а также официальных материалов и неопубликованных документов (научно-исследовательские работы, диссертации), в которых могут содержаться основные вопросы изучаемой проблемы.

Работу с источниками надо начинать с ознакомительного чтения, т.е. просмотреть текст, выделяя его структурные единицы. При ознакомительном чтении закладками отмечаются те страницы, которые требуют более внимательного изучения.

В зависимости от результатов ознакомительного чтения выбирается дальнейший способ работы с источником. Если для разрешения поставленной задачи требуется изучение некоторых фрагментов текста, то используется метод выборочного чтения. Если в книге нет подробного оглавления, следует обратить внимание ученика на предметные и именные указатели.

Избранные фрагменты или весь текст (если он целиком имеет отношение к теме) требуют вдумчивого, неторопливого чтения с «мысленной проработкой» материала. Такое чтение предполагает выделение: 1) главного в тексте; 2) основных аргументов; 3) выводов. Особое внимание следует обратить на то, вытекает тезис из аргументов или нет.

Необходимо также проанализировать, какие из утверждений автора носят проблематичный, гипотетический характер и уловить скрытые вопросы.

Понятно, что умение таким образом работать с текстом приходит далеко не сразу. Наилучший способ научиться выделять главное в тексте, улавливать проблематичный характер утверждений, давать оценку авторской позиции – это сравнительное чтение, в ходе которого студент знакомится с различными мнениями по одному и тому же вопросу, сравнивает весомость и доказательность аргументов сторон и делает вывод о наибольшей убедительности той или иной позиции.

Если в литературе встречаются разные точки зрения по тому или иному вопросу из-за сложности прошедших событий и правовых явлений, нельзя их отвергать, не разобравшись. При наличии расхождений между авторами необходимо найти рациональное зерно у каждого из них, что позволит глубже усвоить предмет изучения и более критично оценивать изучаемые вопросы. Знакомясь с особыми позициями авторов, нужно определять их схожие суждения, аргументы, выводы, а затем сравнивать их между собой и применять из них ту, которая более убедительна.

Следующим этапом работы с литературными источниками является создание конспектов, фиксирующих основные тезисы и аргументы. Можно делать записи на отдельных листах, которые потом легко систематизировать по отдельным темам изучаемого курса. Другой способ – это ведение тематических тетрадей-конспектов по одной какой-



либо теме. Большие специальные работы монографического характера целесообразно конспектировать в отдельных тетрадях. Здесь важно вспомнить, что конспекты пишутся на одной стороне листа, с полями и достаточным для исправления и ремарок межстрочным расстоянием (эти правила соблюдаются для удобства редактирования). Если в конспектах приводятся цитаты, то непременно должно быть дано указание на источник (автор, название, выходные данные, № страницы). Впоследствии эта информация может быть использована при написании текста реферата или другого задания.

Таким образом, при работе с источниками и литературой важно уметь:

- сопоставлять, сравнивать, классифицировать, группировать, систематизировать информацию в соответствии с определенной учебной задачей;
- обобщать полученную информацию, оценивать прослушанное и прочитанное;
- фиксировать основное содержание сообщений; формулировать, устно и письменно, основную идею сообщения; составлять план, формулировать тезисы;
- готовить и презентовать развернутые сообщения типа доклада;
- работать в разных режимах (индивидуально, в паре, в группе), взаимодействуя друг с другом;
- пользоваться реферативными и справочными материалами;
- контролировать свои действия и действия своих товарищей, объективно оценивать свои действия;
- обращаться за помощью, дополнительными разъяснениями к преподавателю, другим студентам.
- пользоваться лингвистической или контекстуальной догадкой, словарями различного характера, различного рода подсказками, опорами в тексте (ключевые слова, структура текста, предваряющая информация и др.);
- использовать при говорении и письме перифраз, синонимичные средства, словоописания общих понятий, разъяснения, примеры, толкования, «словотворчество»;
- повторять или перефразировать реплику собеседника в подтверждении понимания его высказывания или вопроса;
- обратиться за помощью к собеседнику (уточнить вопрос, переспросить и др.);
- использовать мимику, жесты (вообще и в тех случаях, когда языковых средств не хватает для выражения тех или иных коммуникативных намерений).

Подготовка к промежуточной аттестации

При подготовке к промежуточной аттестации целесообразно:

- внимательно изучить перечень вопросов и определить, в каких источниках находятся сведения, необходимые для ответа на них;
- внимательно прочитать рекомендованную литературу;
- составить краткие конспекты ответов (планы ответов).

11. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

Windows 8, Microsoft Office 2007 (Microsoft Word 2007 - Текстовый процессор; Microsoft Excel 2007 - Табличный процессор; Microsoft Access 2007 - Система управления базами данных; Microsoft PowerPoint 2007 - Создание и показ презентаций); ГАРАНТ-Мастер - Информационно-правовая система.

	НОУ ВО «Липецкий эколого-гуманитарный институт»	СИСТЕМА МЕНЕДЖМЕНТА КАЧЕСТВА	
	РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ	РПД-08/2-08-15-2016	
	Информационная безопасность	Взамен РПД - 2015	Стр. 22 из 24

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

Для проведения занятий по дисциплине кафедра располагает необходимой материально-технической базой, обеспечивающей проведение всех видов занятий, предусмотренных данной программой и соответствующей действующим санитарным и противопожарным правилам и нормам:

1. Специализированной аудиторией для проведения лекционных и семинарских занятий, оснащенной ЖК-телевизором, проектором Nec NP-V260G, стационарным экраном «Digis Optimal-C»;

2. Специализированной аудиторией для проведения практических занятий, семинаров, курсового проектирования, консультаций, текущего контроля и промежуточной аттестации, оснащенной ЖК-телевизором, проектором Benq MS504, стационарным экраном «Digis Optimal-C»;

3. Специализированной аудиторией для самостоятельной работы обучающихся, оснащенной ноутбуками «Lenovo B590» с выходом в сеть Интернет и доступом к электронной информационно-образовательной среде ЛЭГИ;

4. Специализированным компьютерным классом, оснащенным ноутбуками «Lenovo B590»;

5. Учебниками, учебными пособиями и методической литературой библиотеки ЛЭГИ, наборами учебно-наглядных пособий по основным разделам программы.



Лист согласования

СОГЛАСОВАНО

РАЗРАБОТАНО

Представитель руководства по СМК

Канд. тех.наук, доцент кафедры ПИЭ

_____ Н.Ю. Филоненко

_____ Р.В. Батищев

« » _____ 2016 г.

« » _____ 2016 г.

