Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 13.10.2023 15:17:46
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ
Декан факультета
информационных технологий
/Д. Г. Демидов/
"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы технологического предпринимательства» в рамках "Проектная деятельность"»

Направление подготовки
10.03.01 «Информационная безопасность»

Профиль
«Безопасность компьютерных систем»

Квалификация
Бакалавр по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):

степень, звание, должность / И.О. Фамилия /

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность», А.Ю. Гневшев

Руководитель образовательной программы, А.Ю. Гневшев

Содержание

1	Цели, задачи и планируемые результаты обучения по дисциплине	4
2	Место дисциплины в структуре образовательной программы	4
3	Структура и содержание дисциплины	4
3.1	Виды учебной работы и трудоемкость	4
3.2	Тематический план изучения дисциплины	5
3.3	Содержание дисциплины	6
3.4	Тематика семинарских/практических и лабораторных занятий	6
3.5	Тематика курсовых проектов (курсовых работ)	6
4	Учебно-методическое и информационное обеспечение	7
4.1	Нормативные документы и ГОСТы	7
4.2	Основная литература	7
4.3	Дополнительная литература	7
4.4	Электронные образовательные ресурсы	7
4.5	Лицензионное и свободно распространяемое программное обеспечение	7
4.6	Современные профессиональные базы данных и информационные справочные системы	7
5	Материально-техническое обеспечение	7
6	Методические рекомендации	7
6.1	Методические рекомендации для преподавателя по организации обучения	7
6.2	Методические указания для обучающихся по освоению дисциплины	8
7	Фонд оценочных средств	8
7.1	Методы контроля и оценивания результатов обучения	8
7.2	Шкала и критерии оценивания результатов обучения	8
7.3	Оценочные средства	8

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины **«Основы технологического предпринимательства»** следует отнести:

- теоретическая и практическая подготовка специалистов в области обеспечения безопасности инноваций (в т. ч., в сфере информационных технологий и информационной безопасности).

К **основным задачам** освоения дисциплины «**Основы технологического предпринимательства**» следует отнести:

- овладение принципами проведения обеспечения информационной и экономической безопасности в сфере инноваций и технологического предпринимательства.

Обучение по дисциплине «Основы технологического предпринимательства» направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК-1. Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	знать: значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	знать: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
ОПК-6. Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	знать: как организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

2 Место дисциплины в структуре образовательной программы

Дисциплина «**Основы технологического предпринимательства**» относится к части, формируемой участниками образовательных отношений (Б1.2) модуль «Проекты и проектная деятельность» (Б1.2.08) основной образовательной программы (Б1.2.05.2).

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОП: «Основы информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **2** зачетные единицы, т.е. **72** академических часа (семинары и практические занятия – 36 часов, самостоятельная работа - 36часов, форма контроля- зачет) в 4 семестре.

Структура и содержание дисциплины «**Основы технологического предпринимательства**» по срокам и видам работы отражены в пунктах 3.1, 3.2 и 3.3.

3.1 Виды учебной работы и трудоемкость (по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**36**	4	1-18
	В том числе:			
1.1	Лекции			
1.2	Семинарские/практические занятия	36	4	1-18
1.3	Лабораторные занятия			
2	**Самостоятельная работа**	**36**	4	1-18
3	**Промежуточная аттестация**		4	19-21
	Зачет			
	Итого:	**72**		

3.2 Тематический план изучения дисциплины (по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/ практические занятия	Лабораторные занятия	Практическая подготовка	
1	Тема 1. Новые технологии и тенденции развития техносферы	4			2		2
2		4			2		2
3		4			2		2
4		4			2		2
5		4			2		2
6		4			2		2

7	Тема 2. Основы противодействие конкурентной разведке и примышленному шпионажу	4			2		2
8		4			2		2
9		4			2		2
10		4			2		2
11		4			2		2
12		4			2		2
13	Тема 3. Защита от внутренних угроз информационной безопасности	4			2		2
14		4			2		2
15		4			2		2
16		4			2		2
17		4			2		2
18		4			2		2
Итого		**72**			**36**		**36**

3.3 Содержание дисциплины

Тема 1. Новые технологии и тенденции развития техносферы

Представление информации и информационные технологии. Революции в образовании и экономика знаний. Знания как информационное оружие. Биоинформатика. Модели для выявления и анализа возможностей, рисков и угроз. Динамические контурные потоки в организации. Управление знаниями, как новая функция управления. Структура и процесс управления знаниями. Основные компоненты УЗ. Источники знаний в компании. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе. Подготовка и планирование внедрения знаний. Внедрение системы управления знаниями и ее развитие. Общение и обучение. Анализ хода реализации проекта.

Тема 2. Основы противодействие конкурентной разведке и примышленному шпионажу

Способы получения и оценки информации. Методы поиска и вербовки информаторов. Методы обеспечения результативного общения. Методы целенаправленного воздействия на человека. Обеспечение безопасности разведывательной работы. Элементы системы безопасности. Внешняя безопасность. Внутренняя безопасность. Локальная безопасность. Организация встреч. Проблемы безопасности бизнесмена. Поиск и обезвреживание взрывных устройств.

Тема 3. Защита от внутренних угроз информационной безопасности

Введение в инсайдерские угрозы. Экосистема внутренних нарушителей: суть проблемы и классификация инсайдеров. Классификация инсайдерских угроз. Нормативная совместимость. Нормативные акты корпоративного управления: Федеральный закон «О

персональных данных». Стандарт Банка России по ИБ Соглашение BaselII Кодекс корпоративного поведения ФСФР. Американский закон SOX Корпоративное управление. Проблема утечки конфиденциальной информации. Методы оценки эффективности в сфере защиты информации от утечек. Организационные меры защиты. Кадровая безопасность. Нетрадиционные методы оценки персонала. Управление изменениями в ИТ-инфраструктуре. Службы обмена мгновенными сообщениями и инсайдеры. Новая парадигма внутренней ИТ-безопасности. Выбор программного средства защиты. Выбор программно-аппаратного средства защиты. Защита от утечек через сменные носители. Проблемы на пути внедрения защиты от утечек. Юридические аспекты Проблемы корпоративного управления правами (ERM) Трудности контентной фильтрации Архивирование электронной корреспонденции. Нормативные акты в сфере архивирования почты Сценарии использования централизованных архивов. Примеры внедрения.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1.
2.
…

4.2 Основная литература

1. Беловицкий К.Б. Экономическая безопасность [Электронный ресурс] : учебное пособие / К.Б. Беловицкий, В.Г. Николаев. — Москва : Научный консультант, 2017. — 286 с. — Режим доступа: https://e.lanbook.com/book/106209
2. Ронин Р. Своя разведка. [Электронный ресурс] -Мн.: Харвест. 2015. -256с. с. — Режим доступа: http://lib100.com/iwar/reconnaissance/doc/
3. .Фирсова О.А. Экономическая безопасность предприятия [Электронный ресурс] : учебно-методическое пособие / О.А. Фирсова.— Орел: , 2014. — 165 с. — Режим доступа: https://e.lanbook.com/book/97734

4.3 Дополнительная литература

1. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефиров С.Л., Голованов В.Б. [Электронный ресурс] - М.:ЦИПСиР, 2011. - 373 с. ISBN 978-5-9614-1364-9 - Режим доступа: http://znanium.com/catalog/product/556539
2. Бержье Ж. Промышленный шпионаж. [Электронный ресурс] -М.: Вузовская книга. 2011 196с.— Режим доступа: http://www.phantastike.com/other/industrial_espionage/zip/
3. Петров М.И. Безопасность и персонал.[Электронный ресурс] -М.: Управление персоналом, 2006. — 240 с.— Режим доступа: https://www.twirpx.com/file/291661/
4. Семененко В.А. Информационная безопасность : учеб. пособие для вузов. - М.: МГИУ, 2010. Гриф УМО.
5. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. [Электронный ресурс] — СПб.: Питер, 2008. — 320 с: — Режим доступа: https://www.livelib.ru/author/211716/top-vladimir-skiba

4.4 Электронные образовательные ресурсы

1. Электронный образовательный ресурс на разработке.
2. ЭБС издательства Лань http://e.lanbook.com/
3. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru/.

4. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.
5. Сайт Федеральной службы безопасности России (ФСБ России). -http://www.fsb.ru.
6. Сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России). http://www.fstec.ru.
7. Портал технического комитета по стандартизации «Защита информации». −http://tk.gost.ru/wps/portal/tk362
8. Информационно-аналитический Интернет-портал ISO27000.ru. −http://www.iso27000.ru/
9. Портал по безопасности. − http://www.sec.ru/.
10. http://www.risk-manage.ru/
11. Операционная система Windows 7(или ниже) – MicrosoftOpenLicense Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215.
12. Офисные приложения, MicrosoftOffice 2013(или ниже) – MicrosoftOpenLicense Лицензия № 61984042.

5 Материально-техническое обеспечение

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, ноутбук, экран) – 1 комплект.

Для проведения практических занятий необходимо наличие компьютерных классов оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

Методические рекомендации по организации обучения по дисциплине могут содержать описание применяемых образовательных технологий, видов учебной работы, методов и форм текущего контроля и промежуточной аттестации.

6.2 Методические указания для обучающихся по освоению дисциплины

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются *лекции.*

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Практические занятия* проводятся по теоретическим и проблемным вопросам ИБ. Практическое занятие предполагает творческие дискуссии, активный обмен мнениями по поставленным *вопросам,* заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю)

оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на экзамене в письменной (устной) форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- подготовка к решению прикладных задач, групповых упражнений;
- подготовка к выполнению практических работ и их защита;
- тест;
- зачет.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю). Шкалы оценивания результатов промежуточной аттестации и их описание:

ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации	Обучающийся демонстрирует неполное соответствие следующих знаний: значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации.Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании	Обучающийся демонстрирует частичное соответствие следующих знаний: значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации,но допускаются незначительные ошибки, неточности,	Обучающийся демонстрирует полное соответствие следующих знаний: значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации, свободно оперирует приобретенными знаниями.

		знаниями при их переносе на новые ситуации.	затруднения при аналитических операциях.	
ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты				
знать: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	Обучающийся демонстрирует неполное соответствие следующих знаний: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их	Обучающийся демонстрирует частичное соответствие следующих знаний: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации,но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации свободно оперирует приобретенными знаниями.

		переносе на новые ситуации.		

ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю				
знать: как организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Обучающийся не владеет или в недостаточной степени владеет способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Обучающийся владеет способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролюв неполном объеме, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, Обучающийся испытывает значительные затруднения при применении навыков в новых ситуациях	Обучающийся частично владеет способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации.	Обучающийся в полном объеме владеет способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю, свободно применяет полученные навыки в ситуациях повышенной сложности.

Форма промежуточной аттестации: зачет

Промежуточная аттестация обучающихся в форме экзамена проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	**Описание**
Зачтено	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Не зачтено	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателей, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Тест-вопросы

Угрозы безопасности компьютерной информации

S: Под угрозой безопасности информации понимается:

-: Атака на информацию со стороны злоумышленника

+: Потенциально возможное событие, процесс или явление, которые могут привести к уничтожению, утрате целостности, конфиденциальности или доступности информации

-: Несанкционированный доступ к информации, который может привести к нарушению целостности системы компьютерной безопасности

S: Все множество потенциальных угроз безопасности информации в КС может быть разделено на следующие классы:

+: Случайные угрозы

-: Потенциальные угрозы

+: Преднамеренные угрозы

-: Предсказуемые угрозы

S: Что понимается под возможным каналом утечки информации?

+: Способ, позволяющий нарушителю получить доступ к хранящейся или обрабатываемой информации

-: Техническое средство, с помощью которого нарушитель может получить доступ к хранящейся или обрабатываемой информации

-: Комплекс программных и/или аппаратных средств, позволяющих осуществлять передачу данных от источника информации к нарушителю

S: С помощью каких типов средств может происходить утечка информации по возможному каналу?

-: Данные

+: Человек

-: Компьютерная сеть

+: Программа

+: Аппаратура

S: При хранении, поддержании и предоставлении доступа к любому информационному ресурсу его владелец, либо уполномоченное им лицо, накладывает явно либо самоочевидно набор правил по работе с ней. Умышленное их нарушение классифицируется как ##### на информацию.

+: атака

S: Перечислите основные виды случайных угроз:

+: Стихийные бедствия и аварии

+: Сбои и отказы технических средств

+: Ошибки при разработке компьютерных систем

+: Алгоритмические и программные ошибки

+: Ошибки пользователей и обслуживающего персонала

-: Электромагнитные излучения и наводки

-: Вредительские программы

S: Перечислите основные виды преднамеренных угроз:

-: Алгоритмические и программные ошибки

+: Шпионаж и диверсии

+: Несанкционированный доступ (НСД) к информации

+: Электромагнитные излучения и наводки

+: Несанкционированная модификация структур

-: Стихийные бедствия и аварии

+: Вредительские программы

S: В зависимости от механизма действия вредительские программы делятся на:

+: Логические бомбы

-: Генераторы белого шума

-: Дизассемблеры

+: Черви

+: Троянские кони

+: Компьютерные вирусы

-: Декомпиляторы

S: К наиболее распространенным методам взлома можно отнести следующие:

-: Подбор пароля с помощью генераторов случайных чисел

+: Доступ к информации через терминалы защищенной информационной системы

+: Получение пароля на основе ошибок администратора и пользователей

+: Получение пароля на основе ошибок в реализации системы

-: Деактивация функций операционной системы (ОС)

+: Социальная психология

+: Комплексный поиск возможных методов доступа

S: Установите соответствие между конкретным методом взлома и классом, к которому он относится.

L1: Социальная психология

L2: Получение пароля на основе ошибок в реализации системы

L3: Получение пароля на основе ошибок администратора и пользователей

L4: Доступ к информации через терминалы защищенной информационной системы

R1: Звонок клиенту от лица администратора

R2: Получение пароля из самой системы

R3: Перебор паролей по словарю

R4: Вход через официальный log-in запрос системы

7.3.2 Список вопросов для зачета

1. Представление информации и информационные технологии. Революции в образовании и экономика знаний.
2. Новые технологии и тенденции развития техносферыБиоинформатика. Биокибернетика. Нанотехнологии.
3. Приоритеты управления и полный вектор управления. Знания как информационное оружие.
4. Модели для выявления и анализа возможностей, рисков и угроз. Прогнозное планирование: определение рисков и поиск возможностей.
5. Методы прогнозирования рисков. Динамические контурные потоки в организации.
6. Управление знаниями. Основные понятия и определения. Управление знаниями, как новая функция управления. Структура системы знаний. Основные компоненты УЗ.
7. Операционно-тактические и стратегические преимущества от применения УЗ в бизнесе. Перспективы применения УЗ в бизнесе. Анализ хода реализации проекта.
8. Нейронные сети, нечеткие множества и интеллектуальные информационные системы
9. Статические и динамические экспертные системы. Приобретение знаний. Извлечение знаний из данных. Источники знаний в компании.Поиск информации в Интернет
10. Нейронные сети. Принципы работы и сфера применения
11. Техносфера и человеко-машинное взаимодействие История ВТ и мультимедиа.
12. Техносфера и человеко-машинное взаимодействие Робототехника и мехатроника.
13. Конкурентная разведка и примышленный шпионаж. Сходство и различие
14. Способы получения и оценки информации Краткая характеристика источников информации. Взятие информации из средств связи. Взятие информации через отслеживание. Использование слухов.
15. Принципы оценки и анализа информации. Достоверность и надежность материалов. Искажение информации и дезинформация. Техника интерпретации данных
16. Выявление и разработка кандидата. Установление и Углубление контакта. Составление досье. Тактика оценки кандидата. Проведение вербовки.
17. Обхождение с завербованным и направление его деятельности. Способы удержания. Способы проверки. Способы связи. Завершение контакта

18. Теория и практика результативного общения. Общие рекомендации по организации. Психофизиологические аспекты. Составные элементы общения. Точность восприятия партнера по общению.
19. Методы обеспечения результативного общения. Методы целенаправленного воздействия на человека. Обеспечение безопасности разведывательной работы
20. Элементы системы безопасности. Обеспечение тайны посланий: криптография. Шифрование. Дешифровка. Стеганография
21. Проблемы безопасности бизнесменаО личном оружии. Требования к телохранителю. Животные-защитники.
22. Проблемы безопасности бизнесмена Общие меры защиты от покушений. Защита автомобиля и квартиры Поведение при похищении. Защита от технических средств.создание своей службы безопасности.
23. Защита от внутренних угроз информационной безопасности. Классификация инсайдеров. Классификация инсайдерских угроз Угроза утечки конфиденциальной информации.
24. Обход средств защиты от утечки конфиденциальной информации. Кража конфиденциальной информации по неосторожности. Нарушение авторских прав на информацию. Мошенничество.
25. Нецелевое использование информационных ресурсов компании. Саботаж ИТ-инфраструктуры. Проблема утечки конфиденциальной информации Портрет респондентов.
26. Внутренние угрозы ИБ. Утечка конфиденциальной информации. Нормативное регулирование. Средства защиты
27. Методы оценки эффективности в сфере защиты информации от утечек
28. Организационные меры защиты Психологические меры. Права локальных пользователей. Стандартизация ПО. Работа с кадрами. Внутрикорпоративная нормативная база.
29. Хранение физических носителей. Система мониторинга работы с конфиденциальной информацией. Аутсорсинг хранения информации
30. Кадровая безопасность Нетрадиционные методы оценки персонала Увольнение работников: Увольнение и трудоустройство уволенных
31. Управление изменениями в ИТ-инфраструктуре Служба ИБ в структуре современной организации.
32. Парадигма внутренней ИТ-безопасности периметральная и канальная защита
33. Средства внутреннего контроля. Системы сильной аутентификации. Предотвращение нецелевого использования ИТ-ресурсов
34. Выбор программного средства защиты от утечек.Службы обмена мгновенными сообщениями и инсайдеры.
35. Выбор аппаратного средства защиты от утечек. Защита от утечек через сменные носители
36. Проблемы на пути внедрения защиты от утечек. Внешние угрозы. Внутренние угрозы.
37. Юридические аспекты. Проблемы корпоративного управления правами (ERM)
38. Решение проблемы резервного копирования. Стимулы к использованию центральных архивов. Требования к системам архивирования. Архивирование интернет-данных.
39. Сценарии использования централизованных архивов Расследование инцидентов ИБ
40. Архивирование электронной корреспонденции. Нормативные акты в сфере архивирования почты Трудности контентной фильтрации