

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 20.10.2023 11:38:28
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ**
Федеральное государственное автономное образовательное учреждение
высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ



Декан факультета
информационных технологий
/Д. Г. Демидов/

августа 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

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

Направление подготовки

10.03.01 «Информационная безопасность»

Образовательная программа (профиль)

«Безопасность компьютерных систем»

Квалификация (степень) выпускника

Бакалавр

Форма обучения

Очная

Год приема - 2021

Москва 2021 г.

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки бакалавров **10.03.01 «Информационная безопасность»**.

Программу составил: доцент, к.т.н. К.В. Пителинский

Программа утверждена на заседании кафедры «Информационная безопасность»
«30» августа 2021 г., протокол № 1.

Заведующий кафедрой
«Информационная безопасность»



к.т.н., доцент

Н.В. Федоров

1. Цели освоения дисциплины

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.

1. Место дисциплины в структуре ОП бакалавриата

Дисциплина «**Основы технологического предпринимательства**» относится к части, формируемая участниками образовательных отношений цикла (Б.1.2) основной образовательной программы (Б.1.2.2.4).

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

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
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	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	безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
--	--	--

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, т.е. 72 академических часа (лабораторные занятия-36 часов, самостоятельная работа -36 часов, форма контроля- зачет) в 7 семестре.

Структура и содержание дисциплины «**Основы технологического предпринимательства**» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины 7 семестр

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 промышленному 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 Basell 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.

5. Образовательные технологии

Методика преподавания дисциплины «**Основы технологического предпринимательства**» и реализация компетентного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению практических работ с использованием видеоуроков;
- проведение интерактивных лекционных и практических занятий в форме видео уроков;
- проведение групповых упражнений;
- обсуждение и защита домашних заданий по дисциплине;
- подготовка, представление и обсуждение презентаций на практических занятиях.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 25% аудиторных занятий. Занятия лекционного типа составляют 50% от объема аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов

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;
- экзамен.

Образцы тестовых заданий, контрольных вопросов для проведения текущего контроля и вопросов к экзамену приведены в приложении.

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

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
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

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
-------	---

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

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 знаниями при их переносе на новые ситуации.	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, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: значения информации в развитии современного общества, применения информационных технологий для поиска и обработки информации, свободно оперирует приобретенными знаниями.
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	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: как принимать	Обучающийся демонстрирует неполное соответствие следующих знаний: как принимать участие в формировании, организовывать и поддерживать выполнение	Обучающийся демонстрирует частичное соответствие следующих знаний: как принимать участие в формировании,	Обучающийся демонстрирует полное соответствие следующих знаний: как принимать участие в формировании, организовывать и

комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации	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 переносе на новые ситуации.	организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации свободно оперирует приобретенными знаниями.
---	--	---	--	---

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 контролю в 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.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) 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>

б) дополнительная литература:

1. Обеспечение информационной безопасности бизнеса / Андрианов В.В., Зефирова 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. Семенов 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>

в) программное обеспечение и интернет-ресурсы:

1. ЭБС издательства Лань —<http://e.lanbook.com/>
2. Научная электронная библиотека eLIBRARY.RU—<http://elibrary.ru/>.

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

8. Материально-техническое обеспечение дисциплины.

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.

9. Методические рекомендации для самостоятельной работы студентов

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. Рекомендуются 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 задания, 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.

10. Методические рекомендации для преподавателя

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

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

Направление подготовки: 10.03.01 «Информационная безопасность»

ОП (профиль): «Безопасность компьютерных систем »

Форма обучения: очная

Вид профессиональной деятельности:

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Основы технологического предпринимательства»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Самостоятельные работы

Тест

Зачет

Составители: доцент, к.т.н. Пителинский К.В.

Москва, 2021 год

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Основы технологического предпринимательства					
ФГОС ВО 10.03.01 «Информационная безопасность»					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие компетенции:					
КОМПЕТЕНЦИИ		Перечень компонентов	Технология формирования компетенций	Форма оценочного средства	Степени уровней освоения компетенций
ИНДЕКС	ФОРМУЛИРОВКА				
ОПК-1	способен оценивать роль информации, информационных технологий 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	лекции, самостоятельная работа, практические занятия	опрос СР, тест зачет	<p>Базовый уровень: демонстрирует полное соответствие следующих знаний: значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации</p> <p>Повышенный уровень: демонстрирует полное соответствие следующих знаний: значение информации в развитии современного общества, применять информационные технологии для поиска информации</p>
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	лекции, самостоятельная работа, практические занятия	опрос СР, тест зачет	<p>Базовый уровень: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности</p> <p>Повышенный уровень: как принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации</p>

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	лекции, самостоятельная работа, практические занятия	опрос СР, тест зачет	<p style="text-align: center;">Базовый уровень:</p> как организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации <p style="text-align: center;">Повышенный уровень:</p> 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
-------	---	---	--	-------------------------------	---

Оценочные средства для текущей аттестации

ТЕСТ-ВОПРОСЫ

по курсу: «Основы технологического предпринимательства»

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
- +: Сбой 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

Оценочные средства для промежуточной аттестации Зачет

Список вопросов для зачета по дисциплине «Основы технологического предпринимательства»

1. Представление информации и информационные технологии. Революции в образовании и экономика знаний.
2. Новые технологии и тенденции развития техносферы. Биоинформатика. 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 промышленный 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 бизнесмена О 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

**Структура и содержание дисциплины «Основы технологического предпринимательства» по направлению подготовки 10.03.01
«Информационная безопасность»
(бакалавр)**

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов	Формы аттестации		
				Л	ПЗ	Лаб	СРС	КСР	К.П. К.Р. ДЗ Реферат	К/р	Э	З
1	Тема 1. Новые технологии и тенденции развития техносферы	7	1	0	0	2	2					
2			2	0	0	2	2					
3			3	0	0	2	2					
4			4	0	0	2	2					
5			5	0	0	2	2					
6			6	0	0	2	2					
7	Тема 2. Основы противодействие конкурентной разведке и промышленному шпионажу		7	0	0	2	2					
8			8	0	0	2	2					
9			9	0	0	2	2					
10			10	0	0	2	2		+			
11			11	0	0	2	2					
12			12	0	0	2	2					
13	Тема 3. Защита от внутренних угроз информационной безопасности		13	0	0	2	2					
14			14	0	0	2	2					
15			15	0	0	2	2					
16			16	0	0	2	2					

17			17	0	0	2	2					
18			18	0	0	2	2					
	<i>Форма аттестации</i>		19-21	0	0	0	0					3
	Всего часов по дисциплине в 7 семестре		144	0	0	36	36					

