МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Кафедра предпринимательства и экономической безопасности

Авторы-составители: **Эстерлейн Жанна Викторовна**
Карпович Юлия Владимировна

Рабочая программа дисциплины

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ БИЗНЕСА

Код УМК 92879

Утверждено
Протокол №10
от «17» мая 2021 г.

Пермь, 2021

1. Наименование дисциплины

Управление информационной безопасностью бизнеса

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в вариативную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.04** Информационно-аналитические системы безопасности
специализация Информационная безопасность финансовых и экономических структур

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Управление информационной безопасностью бизнеса** у обучающегося должны быть сформированы следующие компетенции:

10.05.04 Информационно-аналитические системы безопасности (специализация : Информационная безопасность финансовых и экономических структур)

ПК.2 Способен проводить комплексный анализ угроз экономической безопасности хозяйствующих субъектов

Индикаторы

ПК.2.1 Строит стандартные теоретические и эконометрические модели на основе статистических данных в целях прогнозирования возможных угроз экономической безопасности

4. Объем и содержание дисциплины

Специальность	10.05.04 Информационно-аналитические системы безопасности (специализация: Информационная безопасность финансовых и экономических структур)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	9
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	72
Проведение лекционных занятий	36
Проведение практических занятий, семинаров	36
Самостоятельная работа (ак.час.)	36
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (2)
Формы промежуточной аттестации	Зачет (9 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

Теория и история функции обеспечения безопасности бизнеса. Предмет и система курса.
Понятие безопасности. Генезис функции безопасности в истории общества. Общая теория безопасности и ее взаимодействие со смежными дисциплинами. Зарождение бизнеса и собственно функции обеспечения безопасности предпринимательской деятельности. Особенности перехода от плановой экономики и становления рыночной экономики в новейшей истории России, макроэкономические, политические и иные факторы. Понятие «безопасность предпринимательской деятельности». Цели и задачи обеспечения безопасности бизнеса на современном этапе. Иерархия уровней безопасности. Объекты и субъекты безопасности. Основные подходы к обеспечению безопасности личности, общества и государства в современном мире. Теория безопасности социально-экономических систем. Действующая нормативно-правовая база обеспечения безопасности в Российской Федерации. Предмет и система курса.

Предпринимательские риски и угрозы безопасности бизнеса. Принципы противодействия угрозам, функции системы безопасности
Среда предприятия. Современные системы предпринимательских рисков. Основные виды угроз безопасности предпринимательской деятельности. Единство и взаимосвязь предпринимательских рисков и угроз безопасности бизнеса. Традиционные (линейные) угрозы. Нелинейные угрозы: недобросовестная конкуренция, ограничение конкуренции и насильственное поглощение, промышленный шпионаж, неправомерное применение военных и оперативно-розыскных методов в бизнесе, преступные посягательства на чужую собственность, криминальная идеология и методы, мошеннические действия. Создание финансовых пирамид, получение кредитов без намерений по их возврату. Криминальные, правовые и репутационные риски предприятий и их работников. Коррупционные риски, злоупотребление полномочиями со стороны представителей государственных и муниципальных органов власти. Оценка реальных и потенциальных рисков и угроз. Замысел построения системы безопасности. Анализ внутренней и внешней среды предприятия, особенностей конкурентной борьбы в выбранном сегменте рынка и стандартных угроз. Модель безопасности объекта. Определение приоритетных требований к защите объекта,выбор необходимого и достаточного класса защищенности. Мониторинг угроз безопасности предприятия и действия по их предупреждению и локализации. Функции системы безопасности. Основные профессии штатных сотрудников служб безопасности. «Большой брат» и внешняя среда современного бизнеса, лояльная оценка окружения и поиск путей преодоления конфликтов. Принципы сотрудничества с институтами внешней среды: необходимость, целесообразность, законность.

Промышленный шпионаж
Определение промышленного шпионажа. Уровни промышленного шпионажа, его объекты и субъекты, силы и средства, формы и методы деятельности. Современные возможности проведения операций промышленного шпионажа. Принципы взаимодействия государства и национального бизнеса в области похищения промышленных секретов. Принципы отнесения предприятия к потенциальным объектам промышленного шпионажа. Формирование общих режимов противодействия. Выявление частных случаев промышленного шпионажа, реализованных стремлений к объекту, оценка возможного ущерба и условий, способствовавших реализации целей оппонентов. Частные меры противодействия, использование выявленных технических каналов для
доведения до оппонента недостоверной и фиктивной информации. Общие меры противодействия. Мониторинг защищенности предприятия от промышленного шпионажа, внесение необходимых дополнений и изменений в систему мер по итогам установленных фактов и учебно-тренировочных мероприятий. Особенности подбора персонала

Защита персональных данных, а также сведений, составляющих государственную,

коммерческую, налоговую и банковскую тайны
Философия информационной безопасности бизнеса. Определение информационной безопасности. Информация, ее носители и процессы, подлежащие специальной защите. Государственная тайна и ее защита в реальном секторе экономики. Сведения для служебного пользования, применяемые в органах государственной власти и местного самоуправления. Понятие конфиденциальной информации, информации, содержащей банковскую и налоговую тайну. Защита персональных данных физических лиц. Правила защиты информации на предприятии и кодекс поведения сотрудников, обладающих закрытой информацией

Безопасность электронных ресурсов, систем и процессов
О соотношении понятий информационная и кибернетическая безопасность. Философия информационной безопасности бизнеса. Модели организации кибернетической безопасности предприятия. Построение систем и аудит их эффективности. Проблемы персонала и противодействие угрозам информационной безопасности бизнеса со стороны персонала. Архитектура стандартов защиты информации и принципиальные подходы к их правовому
обеспечению. Взаимодействие службы безопасности (через функцию информационной безопасности) с подразделением ИТ обеспечения предприятия.
Электронные информационные ресурсы, системы и процессы. Типовые сценарии несанкционированного доступа к электронным системам и превентивная защита от них.

Защита бизнеса от внутреннего мошенничества и иных противоправных действий персонала
Определение кадровой безопасности. Концепция безопасного кадрового развития предприятия.Подбор, изучение и принятие решения о зачислении. Возможные кадровые риски, их типология.Примерные правила взаимодействия заинтересованных в приеме специалиста линейных подразделений, подразделений по работе с персоналом и служб безопасности. Психологическая служба, асессмент персонала и детекция лжи. Основные направления обеспечения собственной безопасности компании. Мониторинг персонала. Нисходящие и восходящие коммуникации. Виды и способы выявления фактов мошенничества, похищения чужого имущества, коммерческого подкупа, подлога, намеренно недобросовестного исполнения должностных обязанностей,
пересечения сделок с заинтересованностью, противоречащих корпоративным интересам. Факты недобросовестного исполнения должностных обязанностей, могущие привести к нанесению ущерба компании. Деятельность службы безопасности по выявлению и пресечению внутреннего мошенничества и иных противоправных действий со стороны персонала. Основания и правила проведения внутренних служебных расследований. Конфликты интересов, их предотвращение и локализация. Типология работников, группы риска, методы воздействия на персонал. Процедуры взаимодействия с государственными правоохранительными органами в случае совершения работниками уголовно наказуемых деяний. Основания и правила подготовки заявлений о выявленных фактах противоправных действий лиц и организаций.

Зачет
Знает основные принципы построения системы безопасности
Находит и распознает определения основных понятий курса, применяет знания по работе с информационными
системами

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Турчаева И. Н. Финансовая среда предпринимательства и предпринимательские риски:Учебное пособие/Турчаева И. Н..-Саратов:Вузовское образование,2018, ISBN 978-5-4487-0319-5.-248. http://www.iprbookshop.ru/77575.html

2. Пороткин, Е. С. Инновационная экономика и цифровизация бизнеса : учебное пособие / Е. С. Пороткин. — Самара : Самарский государственный технический университет, 2021. — 132 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/122202

Дополнительная:

1. Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. https://www.iprbookshop.ru/108227

2. Барышева, С. Ю. Защита бизнеса при проверках / С. Ю. Барышева. — Москва : Эксмо, 2009. — 283 с. — ISBN 978-5-699-27040-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/1671

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

www.consultant.ru Консультант плюс
https://rosstat.gov.ru/ Федеральная служба государственной статистики

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

Образовательный процесс по дисциплине **Управление информационной безопасностью бизнеса** предполагает использование следующего программного обеспечения и информационных справочных систем:
1) презентационные материалы (слайды по темам лекционных занятий);
2) доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
3) доступ в электронную информационно-образовательной среду университета;
4) интернет-сервисы и электронные ресурсы.

Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice», Alt Linux.
- ОС "Альт Образование".
- СПС "Консультант Плюс"

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

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

Материально-техническая база обеспечивается наличием:
1. Занятий лекционного типа - аудитория, оснащенная: специализированной мебелью, проектором, ноутбуком/компьютером, экраном, маркерной или меловой доской.
2. Занятий семинарского типа (практические занятия) - аудитория, оснащенная: специализированной мебелью, проектором, ноутбуком/компьютером, экраном, маркерной или меловой доской.
3. Групповые (индивидуальные) консультации, текущий контроль и промежуточная аттестация - Аудитория, оснащенная: аудитория, оснащенная: специализированной мебелью, проектором, ноутбуком/компьютером, экраном, маркерной или меловой доской.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными

компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Управление информационной безопасностью бизнеса

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ПК.2

Способен проводить комплексный анализ угроз экономической безопасности хозяйствующих субъектов

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.2.1 Строит стандартные теоретические и эконометрические модели на основе статистических данных в целях прогнозирования возможных угроз экономической безопасности	умеет разрабатывать рекомендации по построению структуры системы управления рисками владеет навыками построения структуры системы управления рисками с учетом специфики ведения бизнеса знает систему управления рисками. Умеет ориентироваться в различных современных компьютерных программах, обладает практическими навыками их использования, демонстрирует применение современных информационных технологий	**Неудовлетворител** не умеет разрабатывать рекомендации по построению структуры системы управления рисками не владеет навыками построения структуры системы управления рисками с учетом специфики ведения бизнеса не знает систему управления рисками. Не умеет ориентироваться в различных современных компьютерных программах, не обладает практическими навыками их использования, не демонстрирует применение современных информационных технологий **Удовлетворительн** частично сформированное умение разрабатывать рекомендации по построению структуры системы управления рисками. Фрагментарное применение навыков построения структуры системы управления рисками с учетом специфики ведения бизнеса. Общие но не структурированные знания системы управления рисками. Частично сформированное умение ориентироваться в различных современных компьютерных программах, обладает практическими навыками их использования, фрагментарное применение современных информационных технологий **Хорошо** сформированное но содержащее пробелы умение разрабатывать рекомендации по построению структуры системы управления рисками успешное но содержащее пробелы применение навыков построения структуры системы управления рисками с учетом

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо специфики ведения бизнеса сформированные но содержащие пробелы знания системы управления рисками. Сформированное но содержащее пробелы умение ориентироваться в различных современных компьютерных программах, обладает практическими навыками их использования, успешное но содержащее пробелы применение современных информационных технологий, навыков работы с информацией в современных глобальных компьютерных сетях **Отлично** сформированное умение разрабатывать рекомендации по построению структуры системы управления рисками успешное применение навыков построения структуры системы управления рисками с учетом специфики ведения бизнеса сформированные систематические знания системы управления рисками. Сформированное умение ориентироваться в различных современных компьютерных программах, обладает практическими навыками их использования, демонстрирует применение современных информационных технологий успешное применение навыков работы с информацией в современных глобальных компьютерных сетях.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : для ИАСБ

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 43 до 60
«неудовлетворительно» / «незачтено» менее 43 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.2.1 Строит стандартные теоретические и эконометрические модели на основе статистических данных в целях прогнозирования возможных угроз экономической безопасности	Промышленный шпионаж **Письменное контрольное мероприятие**	Определение промышленного шпионажа. Уровни промышленного шпионажа, его объекты и субъекты, силы и средства, формы и методы деятельности. Принципы отнесения предприятия к потенциальным объектам промышленного шпионажа. Формирование общих режимов противодействия. Особенности подбора персонала
ПК.2.1 Строит стандартные теоретические и эконометрические модели на основе статистических данных в целях прогнозирования возможных угроз экономической безопасности	Защита персональных данных, а также сведений, составляющих государственную, коммерческую, налоговую и банковскую тайны **Письменное контрольное мероприятие**	знает определение информационной безопасности. Государственная тайна и ее защита в реальном секторе экономики. Сведения для служебного пользования, применяемые ворганах государственной власти и местного самоуправления. Понятие конфиденциальной информации, информации, содержащей банковскую и налоговую тайну. Правила защиты информации на предприятии и кодекс поведения сотрудников, обладающих закрытой информацией

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.2.1 Строит стандартные теоретические и эконометрические модели на основе статистических данных в целях прогнозирования возможных угроз экономической безопасности	Зачет **Итоговое контрольное мероприятие**	Знать: порядок организации деятельности по управлению информационной безопасностью бизнеса, нормативные акты и стандарты в области управления информационной безопасностью; умеет: выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводить мониторинг. владеет: специализированным программным обеспечением, пониманием структуры и системывзаимосвязи процессов управления информационной безопасностью бизнеса.

Спецификация мероприятий текущего контроля

Промышленный шпионаж

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
Определение промышленного шпионажа. Уровни промышленного шпионажа, его объекты и субъекты, силы и средства, формы и методы деятельности. Принципы отнесения предприятия к потенциальным объектам промышленного шпионажа. Формирование общих режимов противодействия. Особенности подбора персонала	30
Определение промышленного шпионажа. Принципы отнесения предприятия к потенциальным объектам промышленного шпионажа. Формирование общих режимов противодействия. Особенности подбора персонала	24
Определение промышленного шпионажа. Уровни промышленного шпионажа, его объекты и субъекты, силы и средства, формы и методы деятельности.	18
Определение промышленного шпионажа.	13

Защита персональных данных, а также сведений, составляющих государственную, коммерческую, налоговую и банковскую тайны

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **13**

Показатели оценивания	Баллы
знает определение информационной безопасности. Государственная тайна и ее защита в реальном секторе экономики. Сведения для служебного пользования, применяемые в органах государственной власти и местного самоуправления. Понятие конфиденциальной информации, информации, содержащей банковскую и налоговую тайну. Правила защиты информации на предприятии и кодекс поведения сотрудников, обладающих закрытой информацией	30
знает определение информационной безопасности. Понятие конфиденциальной информации, информации, содержащей банковскую и налоговую тайну. Правила защиты информации на предприятии и кодекс поведения сотрудников, обладающих закрытой информацией	24
знает определение информационной безопасности. Государственная тайна и ее защита в реальном секторе экономики. Сведения для служебного пользования, применяемые в органах государственной власти и местного самоуправления.	18
знает определение информационной безопасности. Государственная тайна и ее защита в реальном секторе экономики.	13

Зачет

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Знать: порядок организации деятельности по управлению информационной безопасностью бизнеса, нормативные акты и стандарты в области управления информационной безопасностью; умеет: выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводитьмониторинг. владеет: специализированным программным обеспечением, пониманием структуры и системывзаимосвязи процессов управления информационной безопасностью бизнеса.	40
Знать: порядок организации деятельности по управлению информационной безопасностью бизнеса, нормативные акты и стандарты в области управления информационной безопасностью; владеет: специализированным программным обеспечением, пониманием структуры и системывзаимосвязи процессов управления информационной безопасностью бизнеса.	32
Знать: порядок организации деятельности по управлению информационной безопасностью бизнеса, нормативные акты и стандарты в области управления информационной безопасностью; умеет: выполнять планирование, идентификацию и анализ рисков, моделировать риски, проводитьмониторинг.	24
Знать: порядок организации деятельности по управлению информационной безопасностью	17

бизнеса, нормативные акты и стандарты в области управления информационной безопасностью бизнеса	