Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Максимов Алексей Борисович
Должность: директор департамента по образовательной политике
Дата подписания: 01.11.2023 12:33:42
Уникальный программный ключ:
8db180d1a3f02ac9e60521a5672742735c18b1d6

**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

**УТВЕРЖДЕНО**
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«_28_» __мая_____ 2020 г.

# РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

# «Экономика и управление бизнес процессами в информационной безопасности»

Направление подготовки
**10.05.03 «Информационная безопасность автоматизированных систем»**

Образовательная программа (профиль)
**«Обеспечение информационной безопасности распределенных информационных систем»**

Квалификация (степень) выпускника
**Специалист по защите информации**

Форма обучения
**Очная**

Год приема 2020

Москва 2020 г.

## 1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Экономика и управление бизнес-процессами в информационной безопасности» следует отнести:

- приобретение студентами базовых теоретических знаний и практических навыков по экономическому обоснованию затрат на создание и эксплуатацию технических, организационных и программно-аппаратных средств системы защиты объектов информатизации.

- подготовка студентов к деятельности в соответствии с квалификационной характеристикой специалитета по направлению, в том числе формирование у них умений по выявлению недостатков и оценки эффективности внедрения прогрессивных технологий и средств информационной безопасности.

К **основным задачам** освоения дисциплины «Экономика и управление бизнес-процессами в информационной безопасности» следует отнести:

– освоение методологии анализа и стоимостной оценки ущерба, наносимого владельцу информации, в результате противоправного ее использования, методики оценки затрат на эксплуатацию системы информационной безопасности, технико-экономического обоснования целесообразности инвестиций в комплексные системы защиты информации предприятия.

## 2. Место дисциплины в структуре ООП специалитета.

Дисциплина «Экономика и управление бизнес-процессами в информационной безопасности» относится к числу профессиональных учебных дисциплин базовой части цикла (Б1.1) основной образовательной программы специалитета.
«Экономика и управление бизнес-процессами в информационной безопасности» взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП:

*В базовой части цикла (Б1):*

- Основы информационной безопасности;
- Комплексные системы защиты информации.
- Управление информационной безопасностью

## 3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины 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 |
|---|---|---|
| УК-9 | Способен принимать обоснованные экономические решения в различных областях жизнедеятельности | **знать:**<br>• Основы экономики функционирования предприятия;<br>**уметь:**<br>• Использовать прогрессивные методы и технологии защиты информации в автоматизированных системах;<br>**владеть:**<br>• Инструментом экономического анализа затрат и результатов деятельности предприятия и демонстрировать готовность применения его на практике |
| ПК-5 | Способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | **знать:**<br>• Основные подходы к определению экономического ущерба, нанесенного информации;<br>**уметь:**<br>• Оценивать и оптимизировать затраты по эксплуатации систем и средств защиты информации<br>**владеть:**<br>• Методами определения экономической эффективности внедрения проектных решений в системы безопасности автоматизированных систем и демонстрировать способность и готовность применить их на практике |

## 4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часа (лекции – 36 часов, лабораторные занятия – 36 часов, самостоятельная работа студентов – 72 часа, форма контроля - экзамен) в 8 семестре.

Структура и содержание дисциплины «Экономика и управление бизнес-процессами в информационной безопасности» по срокам и видам работы отражены в приложении.

### Содержание разделов дисциплины

**Задачи экономики и управления бизнес-процессами в информационной безопасности**

Значение, предмет изучения и краткое содержание курса. Методы изучения дисциплины. Научная и периодическая литература. Знания и умения, которые должны быть приобретены студентами в процессе изучения дисциплины. Раскрытие основных экономических понятий, применительно к курсу. Законодательные акты,

регулирующие экономические вопросы защиты информации. Система защиты информации и непрерывность бизнеса предприятия. Подходы к определению затрат на защиту информации. Объем и доля бюджета фирм, выделяемых на ИБ. Анализ структуры затрат, выделяемых на ИБ  Нормативное регулирование построения и функционирование системы защиты информации. ISO/IES 27001-27005

.

**Оценка экономической и информационной безопасности предприятия**

Уровень экономической безопасности предприятия. Задачи экономической безопасности предприятия. Функциональные критерии экономической безопасности предприятия. Внутренние и внешние угрозы производственной деятельности предприятия. Информация как важный ресурс предприятия. Особенности экономической информации о продукции, определение целесообразности ее защиты на разных этапах жизненного цикла. Рынок информационных продуктов и услуг.

**Анализ и страхование рисков**

Этапы построения системы информационной безопасности предприятия. Этап технико-экономической оценки разработанного проекта защиты информации. Анализ угроз и оценка рисков информационной безопасности. Оценка ущерба от риска потери информации. Прямой и косвенный ущерб. Понятие упущенной выгоды предприятия. Оценка риска по двум и трем факторам. Управление рисками. Модель безопасности с полным перекрытием. Программные продукты для анализа и управления рисками.

Страхование рисков информационной безопасности. Способы воздействия на риск. Виды страхования в рамках системы защиты информации.

**Ресурсы предприятия и служб защиты информации.**

Задачи оценки и планирования производственных затрат. Затраты на создание средств защиты информации Нормативное регулирование оценки затрат на основные средства. Единовременные и текущие затраты на основные средства. Первоначальная и остаточная стоимость основного средства. Понятие амортизации. Методы амортизации. Затраты на ремонт.  Понятие нематериального актива. Затраты на приобретение и эксплуатацию нематериального актива. Оборотные средства. Трудовые ресурсы систем защиты информации. Прямые и косвенные расходы службы защиты предприятия. Экономические результаты деятельности фирмы.

**Оценка затрат на создание программных средств защиты информации**

Методика оценки затрат на создание и эксплуатацию программных средств защиты информации. Оценка экономической эффективности программных средств защиты информации

**Методы оценки целесообразности затрат на систему информационной безопасности**

Принципы разумной достаточности при создании системы защиты информации. Связь затрат на информационную безопасность и уровня достигаемой защищенности предприятия. Методы оценки целесообразности затрат на систему информационной безопасности (AIE), (CI), (EVA), (PM), (BSC). Понятие и оценка совокупной стоимости владения информационной системы и системы безопасности (TCO). Перечень затрат на планирование, разработку, внедрение и управление КСЗИ.

**Эффективность капиталовложений в создание средств ЗИ**

Показатели обоснования выбора инвестиционного проекта комплексной системы защиты информации. Учет факторов неопределенности и рисков при оценке эффективности проекта построения КСЗИ. Метод оценки устойчивости проекта. Метод формального описания неопределенности проекта. Выбор и создание системы защиты информации с использованием ФСА.

## 5. Образовательные технологии.

Методика преподавания дисциплины «Экономика и управление бизнес-процессами в информационной безопасности» и реализация компетентностного 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:

– обсуждение и защита рефератов по дисциплине;

– подготовка, представление и обсуждение презентаций по темам рефератов на семинарских занятиях;

– организация и проведение текущего контроля знаний студентов в форме бланкового тестирования;

– проведение интерактивных занятий по процедуре подготовки к интернет-тестированию на сайтах: *i-exam.ru, fepo.ru;*

– использование интерактивных форм текущего контроля в форме аудиторного и внеаудиторного интернет-тестирования;

– проведение мастер-классов экспертов и специалистов по методам и средствам мониторинга, аудита и оценки затрат на функционирования системы защиты информации.

Удельный вес занятий, проводимых в интерактивных формах, определен главной целью образовательной программы, особенностью контингента обучающихся, содержанием дисциплины «Экономика и управление бизнес-процессами в

информационной безопасности» и в целом по дисциплине составляет 25% аудиторных занятий. Занятия лекционного типа составляют 40% 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 и выступление на семинарском занятии с презентацией и обсуждением на тему «Оценка затрат на внедрение средств защиты информации» (индивидуально для каждого обучающегося);
- реферат по теме: «Методы оценки целесообразности затрат на систему информационной безопасности» (AIE), (CI), (EVA), (PM), (BSC) (индивидуально для каждого обучающегося);

Оценочные средства текущего контроля успеваемости включают контрольные вопросы и задания в форме бланкового и (или) компьютерного тестирования, контрольные работы для контроля освоения обучающимися разделов дисциплины.

Образцы тестовых заданий, контрольных работ для проведения текущего контроля, вопросов к зачету, 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 |
|---|---|
| УК-9 | Способен принимать обоснованные экономические решения в различных областях жизнедеятельности |
| ПК-5 | Способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности |

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.

| **УК-9 Способен принимать обоснованные экономические решения в различных областях жизнедеятельности** | | | | |
|---|---|---|---|---|
| **Показатель** | **Критерии оценивания** | | | |
| | **2** | **3** | **4** | **5** |
| **знать:** •Основы экономики функционирования предприятия; | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие знаний об экономической деятельности и экономической безопасности предприятия | Обучающийся демонстрирует неполное соответствие следующих знаний: -допускает значительные затруднения по определению ряда экономических показателей использования активов предприятия, -частично владеет подходами к определению особенностей экономической безопасности деятельности предприятия | Обучающийся демонстрирует частичное соответствие следующих знаний: -владеет основными подходами к определению экономических показателей использования активов предприятия, методами оценки экономической деятельности, но допускаются незначительные ошибки, неточности, затруднения при аналитических ситуациях. | Обучающийся демонстрирует полное соответствие следующих знаний: -владеет методами оценки экономической деятельности и безопасности предприятия и свободно оперирует приобретенными знаниями. |
| **уметь:** Использовать прогрессивные методы и технологии защиты информации в автоматизированных системах; | Обучающийся не умеет или в недостаточной степени умеет использовать технологии защиты информации | Обучающийся демонстрирует неполное соответствие следующих умений: -допускаются существенные ошибки при использовании методов и применении технологий защиты информации в АИС. | Обучающийся демонстрирует частичное соответствие следующих умений: - обосновывается выбор методов и технологий защиты информации но допускает незначительные ошибки, неточности, затруднения при аналитических | Обучающийся демонстрирует полное соответствие следующих умений: обосновывается выбор методов и технологий защиты информации |

| | | | | |
|---|---|---|---|---|
| | | -обучающийся испытывает значительные затруднения при обосновании целесообразности внедрения средств защиты при их использовании в новых ситуациях | операциях, переносе умений на новые, нестандартные ситуации. | -свободно оперирует приобретенным умениями, применяет их в ситуациях повышенной сложности. |
| **владеть:** Инструментом экономического анализа затрат и результатов деятельности предприятия и демонстрировать готовность применения его на практике | Обучающийся не владеет или в недостаточной степени владеет методами анализа затрат и результатов деятельности предприятия | Обучающийся владеет методами анализа и методиками анализа результатов деятельности предприятия и служб в неполном объеме, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду методик испытывает значительные затруднения при применении навыков в новых ситуациях. | Обучающийся частично владеет методами анализа затрат и результатов деятельности предприятия и служб защиты, навыки освоены, но допускаются незначительные ошибки, затруднения при переносе умений на новые, нестандартные ситуации. | Обучающийся в полном объеме владеет методами анализа затрат и результатов деятельности предприятия и служб защиты, свободно применяет полученные навыки в ситуациях повышенной сложности. |
| **ПК-5 Способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности** | | | | |
| **знать:** Основные подходы к определению экономического ущерба, нанесенного информации; | Обучающийся демонстрирует полное отсутствие или недостаточное соответствие знаний для определения экономического ущерба, нанесенного бизнесу предприятия, в результате произошедшего нарушения системы защиты информации | Обучающийся демонстрирует неполное соответствие следующих знаний:<br>-допускает значительные затруднения по определению ряда экономических показателей,<br>-частично владеет подходами к оценке экономического ущерба для бизнеса предприятия, понесенного в результате утечки информации. | Обучающийся демонстрирует частичное соответствие следующих знаний:<br>-владеет основными подходами к определению экономического ущерба, нанесенного информации, но допускаются незначительные ошибки, неточности, затруднения при аналитических ситуациях. | Обучающийся демонстрирует полное соответствие следующих знаний:<br>-владеет основными подходами к определению экономического ущерба, нанесенного информации и свободно оперирует приобретенными знаниями. |

| | | | | |
|---|---|---|---|---|
| **уметь:** Оценивать и оптимизировать затраты по эксплуатации систем и средств защиты информации | Обучающийся не умеет или в недостаточной степени умеет выполнять расчеты по оценке затрат по эксплуатации систем и средств защиты информации | Обучающийся демонстрирует неполное соответствие следующих умений: -допускаются существенные ошибки при выполнении расчетов по оценке затрат на эксплуатацию систем и средств защиты информации. -обучающийся испытывает значительные затруднения при оперировании показателями при их переносе на новые ситуации- | Обучающийся демонстрирует частичное соответствие следующих умений: -выполнять расчеты по оценке затрат по эксплуатации систем и средств защиты информации, но допускает незначительные ошибки, неточности, затруднения при аналитических операциях, переносе умений на новые, нестандартные ситуации. | Обучающийся демонстрирует полное соответствие следующих умений: - выполняет расчеты по оценке затрат на эксплуатацию системы защиты информации. -свободно оперирует приобретенным умениями, применяет их в ситуациях повышенной сложности. |
| **владеть:** Методами определения экономической эффективности внедрения проектных решений в системы защиты информации и демонстрировать способность и готовность применить их на практике | Обучающийся не владеет или в недостаточной степени владеет методами и методиками определения экономической эффективности внедрения мер и средств защиты информации | Обучающийся владеет методами и методиками расчета эффективности внедрения средств защите информации в неполном объеме, допускаются значительные ошибки, проявляется недостаточность владения навыками по ряду показателей, испытывает значительные затруднения при применении навыков в новых ситуациях. | Обучающийся частично владеет методами и методиками расчета эффективности внедрения средств и методов защиты информации, навыки освоены, но допускаются незначительные ошибки, затруднения при переносе умений на новые, нестандартные ситуации. | Обучающийся в полном объеме владеет методами и методиками расчета себестоимости продукции, свободно применяет полученные навыки в ситуациях повышенной сложности. |

Шкалы оценивания результатов промежуточной аттестации и их описание:

***Форма промежуточной аттестации: экзамен.***

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** |
|---|---|

| | |
|---|---|
| Отлично | 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. |
| Хорошо | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки. |
| Удовлетворительно | Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность. |
| Неудовлетворительно | 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. Артемов А.В. Информационная безопасность: курс лекций. Орел: МАБИВ, 2016- Режим доступа -http://biblioclub.ru
2. Гребенников П.И Экономика. Учебник для академического бакалавриата. СПб:Питер, 2019.
3. Мельников В.В. Государственное регулирование национальной экономики. Учебное пособие. М.: Омега-Л, 2015.


### б) дополнительная литература:


1. Ларина И.Е. Экономика защиты информации. Учебное пособие.; МГИУ, 2010 г
2. Плашенков В.В. Обеспечение безопасности бизнеса промышленных предприятий : теория и практика: учебное пособие. Издательство ЧГУ , 2014 г. -Режим доступа - http://biblioclub.ru
3. Семененко В.А. Информационная безопасность : учеб. пособие для вузов. - М.: МГИУ, 2010 г.

**в) программное обеспечение и интернет-ресурсы:**

Программное обеспечение не предусмотрено

Полезные учебно-методические и информационные материалы представлены на сайтах:

**1. ИТ-портал компании «Инфосистемы джет» -Режим доступа - http://www.jetinfo.ru**

**2. «Информационная безопасность», журнал – Режим доступа - http://itsec.ru/imag/**

## 8. Материально-техническое обеспечение дисциплины.

Проведение лекционных и практических осуществляется в мультимедийной аудитории

## 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.* При рассмотрении учебного материалы рекомендуется делать акцент на структуру и взаимосвязь аспектов безопасности - методологии, информационного обеспечения, организации, экономических методах, кадрового обеспечения и нормативно-правовой базы. Полезно также сосредоточить внимание студентов на анализе угроз и оценке рисков информационной безопасности, оценке прямого и косвенного ущерба от риска потери информации, определении упущенной выгоды предприятия, методах оценки целесообразности и эффективности затрат на систему информационной безопасности

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, дорабатывают конспекты лекций, готовятся к зачету, а также самостоятельно изучают отдельные темы учебной программы. В тематическом плане указанные темы выделены курсивом и снабжены пометкой «самостоятельно». Преподаватель направляет самостоятельную работу студентов, отвечает на возникающие вопросы, дает рекомендации по методике изучения тем.

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 экзамене.

Самостоятельная работа по дисциплине «Экономика и управление бизнес-процессами в информационной безопасности» 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 в 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 устной форме.

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;

- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность умений;
- оформление материала в соответствии с требованиями.

## 10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки специалист **10.05.03 «Информационная безопасность автоматизированных систем».**

**Программу составил:**

доцент, к.э.н. Ларина И.Е.

**Программа утверждена на заседании кафедры "Информационная безопасность"** «28» мая 2020 г., протокол № 1

Заведующий кафедрой
доцент, к. т. н. /Н.В.Федоров/

Приложение 1

**Структура и содержание дисциплины «Экономика и управление бизнес-процессами в информационной безопасности»**
**по направлению подготовки**
**10.05.03 «Информационная безопасность автоматизированных систем»**
**(специалист)**

| n/n | Раздел | Семестр | Неделя семестра | Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах | | | | | Виды самостоятельной работы студентов | | | | | Формы аттестации | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Л | П/С | Лаб | СРС | КСР | К.Р. | К.П. | РГР | Реферат | К/р | Э | З |
| | **8семестр** | | | | | | | | | | | | | | |
| **1.1** | **Задачи экономики защиты информации** | **8** | **1-2** | **4** | | | **4** | | | | | | | | |
| **1.2** | *Семинарское занятие* Нормативное регулирование построения и функционирование системы защиты информации | **8** | **1-2** | | | **4** | **4** | | | | | | | | |
| **1.3** | **Оценка экономической и информационной безопасности предприятия** | **8** | **3-4** | **4** | | | **4** | | | | | | | | |
| **1.4** | *Семинарское занятие* Функциональные критерии экономической безопасности предприятия | **8** | **3-4** | | | **4** | **4** | | | | | | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1.5** | **Анализ и страхование рисков** | **8** | **5-6** | **4** | | | **4** | | | | | | | | |
| **1.6** | *Семинарское занятие* Методики оценки рисков GRAMM и FRAM | **8** | **5** | | | **2** | **4** | | | | | | | | |
| **1.7** | *Семинарское занятие* Страхование рисков информационной безопасности | **8** | **6** | | | **2** | **4** | | | | | | | | |
| **1.8** | **Ресурсы предприятия и служб защиты информации** | **8** | **7-10** | **8** | | | **4** | | | | | | | | |
| **1.9** | *Семинарское занятие* Производственные и информационные ресурсы предприятия. Основные средства | **8** | **7-8** | | | **4** | **4** | | | | | | | | |
| **1.10** | *Семинарское занятие* Производственные и информационные ресурсы предприятия. Нематериальные активы Оборотные средства | **8** | **9** | | | **2** | **4** | | | | | | | | |
| **1.11** | *Семинарское занятие* Производственные и информационные ресурсы предприятия. Трудовые ресурсы систем защиты информации. Экономические результаты деятельности фирмы *Контрольная работа* | **8** | **10** | | | **4** | **4** | | | | | | **+** | | |
| **1.12** | **Оценка затрат на создание программных средств защиты информации** | 8 | **11-12** | **4** | | | **6** | | | | | | | | |

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1.13** | *Семинарское занятие.* Затраты на создание средств защиты информации | **8** | **11-12** | | | **4** | **4** | | | | | | | | |
| **1.14** | **Методы оценки целесообразности затрат на систему информационной безопасности** | **8** | **13-14** | **6** | | | **4** | | | | | | | | |
| **1.15** | *Семинарское занятие* Методы оценки затрат на функционирование системы ИБ<br>*Задание на реферат* | **8** | **13-14** | | | **4** | **4** | | | | | + | | | |
| **1.16** | **Эффективность капиталовложений в создание средств ЗИ** | **8** | **15-17** | **6** | | | **4** | | | | | | | | |
| **1.17** | *Семинарское занятие* Расчет эффективности капиталовложений в информационную безопасность<br>*Контрольная работа* | **8** | **15-16** | | | **4** | **4** | | | | | | + | | |
| **1.18** | *Итоговое семинарское занятие* | **8** | **17** | | | **2** | **2** | | | | | | | | |
| | ***Форма аттестации*** | | | | | | | | | | | | | **З** | |
| | ***Всего часов по дисциплине***<br>***В семестре*** | | | **36** | | **36** | **72** | | | | | Один | Две | | |

Приложение 2

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетноеобразовательное учреждение высшего образования
**«Московский политехнический университет»**
**(МОСКОВСКИЙ ПОЛИТЕХ)**

Направление подготовки: **10.05.03 «Информационная безопасность автоматизированных систем»**
Профиль «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная
Вид профессиональной деятельности: научно-исследовательская; проектно-конструкторская; контрольно-аналитическая; организационно-управленческая; эксплуатационная

Кафедра: Информационная безопасность

# ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
# ПО ДИСЦИПЛИНЕ «Экономика и управление бизнес-процессами в информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
___рефераты_____
____контрольные работы___
_____тесты_____

**Составители:** **доц. Ларина И.Е**

Москва, 2020 год

Таблица 1

## ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

| **Экономика и управление бизнес-процессами в информационной безопасности** | | | | | |
|---|---|---|---|---|---|
| ФГОС ВО **10.05.03 «Информационная безопасность»** | | | | | |
| В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общекультурные компетенции**: | | | | | |
| **КОМПЕТЕНЦИИ** | | **Перечень компонентов** | **Технология формирования компетенций** | **Форма оценочного средства** | **Степени уровней освоения компетенций** |
| **ИНДЕКС** | **ФОРМУЛИРОВКА** | | | | |

| | | | | | |
|---|---|---|---|---|---|
| УК-9 | Способен принимать обоснованные экономические решения в различных областях жизнедеятельности | знать:<br>•Основы экономики функционирования предприятия;<br>уметь:<br>Использовать прогрессивные методы и технологии защиты информации в автоматизированных системах;<br>владеть:<br>Инструментом экономического анализа затрат и результатов деятельности предприятия и демонстрировать готовность применения его на практике | лекция, самостоятельная работа, семинарские занятия | УО,<br>К/Р, Т,<br>Р | Базовый уровень<br>- способен использовать экономические знания в области обоснования целесообразности применяемых мер и средств обеспечения информационной безопасности<br>Повышенный уровень<br>- применять инструменты экономического анализа затрат и результатов деятельности предприятия и служб защиты информации |

| | | | | | |
|---|---|---|---|---|---|
| ПК-5 | Способен проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности | знать:<br><br>Основные подходы к определению экономического ущерба, нанесенного информации;<br><br>уметь:<br><br>Оценивать и оптимизировать затраты по эксплуатации систем и средств защиты информации<br><br>владеть:<br><br>Методами определения экономической эффективности внедрения проектных решений в системы защиты информации и демонстрировать способность и готовность применить их на практике | лекция, самостоятельная работа, семинарские занятия | УО,<br><br>К/Р, Т,<br><br>Р | Базовый уровень<br><br>- способен экономически обосновывать принимаемые проектные решения по внедрению отдельных средств защиты информации<br><br>Повышенный уровень<br><br>- способен анализировать исходные данные и участвовать в технико-экономическом обосновании проектных решений по созданию КСЗИ и оценке эффективности принимаемых проектных решений |

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

### 1. Контрольные вопросы к зачету по дисциплине

1. Экономические проблемы защиты информационных ресурсов предприятия
2. Уровень экономической безопасности предприятия
3. Внешние и внутренние угрозы производственной деятельности предприятия
4. Функциональные составляющая экономической безопасности предприятия
5. Частные функциональные критерии экономической безопасности предприятия
6. Информация как важный ресурс экономики
7. Характеристика информации и информационных рынков, как стратегически важный объект государственного регулирования
8. Понятие информационных ресурсов предприятия
9. Конфиденциальная информация и сведения, представляющие собой коммерческую тайну
10. Задачи экономики защиты информации
11. Порядок построения и экономическое обоснование создания системы защиты информации
12. Этапы построения КСЗИ
13. Этап предварительного обследования состояния объекта и уровня организации защиты информации
14. Этап выявления потенциальных угроз и оценка вероятностей их появления
15. Оценка состояния действующей на предприятие системы информационной безопасности
16. Этап определения задач защиты информации и определения мер по их реализации
17. Технико-экономическое обоснование проекта КСЗИ
18. Анализ угроз и оценка рисков информационной безопасности
19. Понятие объективных и субъективных угроз безопасности конфиденциальной информации предприятия
20. Экономические последствия несанкционированного доступа к информации
21. Модель нарушителя информационной безопасности предприятия
22. Классификация затрат на создание и эксплуатацию КСЗИ
23. Оценка ущерба от риска потери информации на предприятие
24. Оценка риска потери информации по двум факторам
25. Оценка риска потери информации по трем факторам
26. Экспертные системы управления информационной безопасностью предприятия
27. Страхование рисков как способ экономической защиты информации
28. Виды страхования в рамках системы защиты информации. Страхование имущества.
29. Виды страхования в рамках системы защиты информации. Страхование ответственности
30. Виды страхования в рамках системы защиты информации. Личное страхование
31. Характеристика производственных ресурсов предприятия и служб защиты информации
32. Задачи оценки и планирования производственных затрат служб защиты информации
33. Оценка затрат на основные средства системы защиты информации
34. Затраты на амортизацию и ремонт инженерно-технических и аппаратных средств защиты информации
35. Затраты на нематериальные активы
36. Оценка затрат на разработку программных средств ЗИ
37. Ценообразование интеллектуального продукта
38. Понятие оборотных средств системы и служб защиты информации Оценка затрат на

оборотные средства
39. Затраты на трудовые ресурсы КСЗИ
40. Результаты деятельности фирмы Формирование себестоимости и прибыли предприятия
41. Основные подходы к оценке эффективности создания средств ЗИ
42. Сравнительные показатели экономической эффективности альтернативных вариантов КСЗИ
43. Показатели оценки экономической эффективности внедрения КСЗИ
44. Расчет капитальных затрат на разработку, внедрение и эксплуатацию КСЗИ
45. Показатели эффективности инвестиционных проектов
46. Показатели обоснования выбора инвестиционных проектов КСЗИ
47. Учет факторов неопределенности и рисков при оценке эффективности проекта построения КСЗИ
48. Метод проверки устойчивости проекта
49. Метод формального описания неопределенности проекта
50. Выбор и создание системы ЗИ с использованием ФСА

## 2.Примерная тематика рефератов по курсу «Экономика и управление бизнес-процессами в информационной безопасности»

2.1 Подготовка и выступление на семинарском занятии с презентацией и обсуждением на тему «Оценка затрат на внедрение средств защиты информации» (программных, программно-аппаратных, технических, инженерных, организационных).

2.2 Реферат по теме: «Зарубежные методики оценки целесообразности затрат на систему информационной безопасности» (AIE), (CI), (EVA), (PM), (BSC).

## 3.Тестовые вопросы по курсу «Экономика и управление бизнес-процессами в информационной безопасности»

1. Что понимается под прибылью предприятия при создании и эксплуатации систем информационной безопасности?

а. Разница, полученная предприятием, между выручкой и себестоимостью произведенной продукции, работ и услуг

б. Количественная оценка уменьшения потерь информации от предотвращения действия угрозы

в. Количественная оценка уменьшения потерь информации от предотвращения действия угрозы плюс реализационная прибыль от продажи произведенной продукции, работ и услуг.

2. Экономическое обоснование затрат на создание и эксплуатацию технических и программных средств защиты необходимо

а . для оценки эффективности принятых мер по защите информации на предприятии

б. для сокращения доли бюджета предприятий, выделяемую на собственную безопасность

в. для обоснования оптимальной структуры и состава системы зашиты информации на предприятии

3. Экономический эффект от использования системы защиты информации определяется

а . исходя из анализа и классификации рисков, возникающих при защите информации
б. на основе экспертных оценок уровня, понесенного или предотвращенного ущерба в результате внедрения КСЗИ
в. на основе оценки затрат на создание и эксплуатацию комплексной системы защиты информации и стоимости уровня, понесенного и/или предотвращенного ущерба

4. На каком этапе построения системы информационной безопасности оценивается эффективность КСЗИ
а . на этапе обоснования структуры и технологии функционирования КСЗИ
б. на этапе технико-экономической оценки разрабатываемого проекта КСЗИ
в. на этапе обоснования задач защиты информации и определения необходимых мер обеспечения информационной безопасности на предприятии

5. Необходимым условием обоснования эффективности создания и функционирования системы информационной безопасности является
а . анализ угроз информационной безопасности предприятия
б. проведение аудита состояния информационной безопасности предприятия
в. анализ угроз и оценка состояния информационной безопасности предприятия

6. Уровень экономической безопасности предприятия по информационной составляющей определяется
а. как отношение общего понесенного ущерба экономической безопасности предприятия к предотвращенному ущербу за период
б. как отношение общего предотвращенного ущерба экономической безопасности предприятия к понесенному ущербу и затратам на обеспечение информационной безопасности на предприятии за анализируемый период
в. как отношение общего понесенного ущерба экономической безопасности предприятия и затратам на обеспечение информационной безопасности на предприятии к предотвращенному ущербу за анализируемый период

7. Ущерб от различных рисков потери информации включает
а. прямые и косвенные убытки
б упущенную выгоду предприятия от простоя атакованного узла
в. прямые убытки от понесенного ущерба

8. При оценке рисков информационной безопасности не по двум, а по трем факторам какой дополнительный фактор учитывается
а. цена потери
б. вероятность происшествия
в. вероятность угрозы

9. К какому способу воздействия на риск относится способ страхование рисков
а. исключение риска
б. снижения вероятности возникновения риска
в. сохранение существующего уровня риска

10 . В каких случаях применяется страхование как дополнительная мера защиты информации
а. когда других мер по обеспечению безопасности недостаточно
б. когда другие меры непригодны или слишком дороги
в. когда вероятность реализации угрозы не очень велика, но последствия для информационной системы незначительны.

11. Какие виды страхования в рамках системы защиты информации возможны
а. страхование имущества и личное страхование
б. страхование имущества, ответственности и личное страхование
в. страхование имущества и ответственности

12 Какие производственные затраты оцениваются при оценке эффективности построения системы информационной безопасности
а . затраты на основные средства, нематериальные активы, материалы и трудовые ресурсы
б. затраты на основные средства, программное обеспечение, трудовые ресурсы
в. затраты на программное и аппаратное обеспечение системы информационной безопасности предприятия

13 Как оцениваются затраты на технические средства в процессе эксплуатации системы безопасности предприятия
а. путем расчета амортизационных отчислений на восстановление стоимости технических средств
б. путем определения срока полезного использования и расчета амортизационных отчислений на восстановление стоимости технических средств
в. затраты на технические средства в процессе эксплуатации технических средств не рассчитываются.

14 Как оцениваются затраты на программные средства используемые в процессе эксплуатации системы безопасности предприятия
а. путем расчета амортизационных отчислений на восстановление стоимости программного обеспечения
б. путем определения срока полезного использования и расчета амортизационных отчислений на восстановление стоимости программного обеспечения
в. затраты на программные средства оцениваются только в период их приобретения

15. Какие показатели используются для оценки эффективности КСЗИ
а. условно-годовая экономия от внедрения КСЗИ, затраты на создание КСЗИ
б. фактический срок окупаемости и коэффициент эффективности КСЗИ
в. годовой экономический эффект и фактический срок окупаемости

16. Можно ли рассматривать годовую экономию от внедрения КСЗИ как предполагаемый ущерб, которое предприятие могло бы понести в случае утечки информации?
а. да
б. нет

17. Когда инвестиционный проект в систему защиты информации является эффективным
а. когда чистый дисконтированный доход > 1
б. когда чистый дисконтированный доход < 1
в. когда индекс доходности <1

18. Для чего используется Функционально-стоймостной анализ при построении КСЗИ на предприятии
а. используется как метод снижения затрат при создании системы информационной безопасности предприятия
б используется как метод снижения затрат и оптимизации структуры системы информационной безопасности предприятия

в. используется как метод снижения затрат, оптимизации структуры и выполняемых функций системы информационной безопасности предприятия

## 4. Варианты контрольных работ

**Контрольная работа на тему «Определение упущенной выгоды предприятия в результате произошедшего инцидента нарушения информационной безопасности**

**Вариант задания.** Производственные и информационные ресурсы предприятия и средств защиты информации

*Вариант задания.*

*Задание 1*. Ежемесячный объем производства дефицитной продукции фирмой «Одуванчик» составляет 10000 шт. Затраты на производство за месяц составляют:

| | |
|---|---|
| 1 . Сырье и материалы | 43 000 руб. |
| 2. Заработная плата | 125 000 руб. |
| 3. Амортизация оборудования | 12 000 руб. |
| 4. Амортизация нематериальных активов | 300 руб. |
| 5. Услуги вспомогательных производств | 24 000 руб. |
| 7. Общехозяйственные расходы | 8 000 руб. |

Весь объем выпускаемой продукции реализуется Затраты на упаковку единицы произведенной продукции составили 12 руб.02 коп. Цена реализации единицы продукции составляет. 80 рублей за штуку.

В июне произошла утечка информации, в результате которой предприятию не удалось реализовать 30 % произведенной продукции, а на реализованную продукцию была снижена цена на 10%

Предприятием в июне проведены дополнительные мероприятия по обеспечению безопасности обрабатываемых данных. Приобретена и установлена компьютерная программная система идентификации и аутентификации пользователей «Панцирь-К» стоимостью 280 000 руб. Затраты по установке и запуску системы составили 40 000 руб., на обучение персонала 15 000 руб.

В июле вновь выпущенная продукция в размере 10000 шт. и остатки продукции нереализованной в июне проданы по новой цене. При этом предприятие «Лютик» понесло дополнительные затраты по транспортировке всей партии проданной продукции заказчику в размере 7 000 руб.

Определить себестоимость единицы продукции произведенной в июне и июле, полученную прибыль предприятия «Одуванчик» за два месяца и упущенную выгоду, если бы утечки информации не произошло и мероприятия по обеспечению безопасности не производились

*Задание 2*

Перечислите методы расчета стоимости материалов при списании их в производство

**Контрольная работа 2.** Оценка эффективности инвестиций в систему защиты информации

**Вариант задания**

*Задание 1*

Оцените себестоимость разработки программных средств защиты информации. Разработка осуществлялась в течение 2 месяцев коллективом из 4 программистов на 4-х выделенных для разработки ПЭВМ.

В процессе разработки затраты материалов составили 1500 руб. в месяц. Основная заработанная плата программистов в месяц – 15000 руб., прогрессивные доплаты в месяц составили 25 % к основной зарплате. годовой действительный фонд времени работы 1-ой ЭВМ составляет 3000 часов, цена приобретения 1-ой ЭВМ 30000 руб., годовая норма амортизации – 25%; стоимость системного программного обеспечения равна 35000 руб., годовая норма амортизации СПО 20%; зарплата обслуживающего персонала ЭВМ численностью 1 человек 12000 руб. в месяц.; норма обслуживания 15 ПЭВМ; стоимость программного обеспечения по обслуживанию ЭВМ - 15000 руб., норма амортизации – 25% в год; паспортная мощность ЭВМ - 3 квт., цена 1 квт/ч – 4,0 руб.; общие накладные расходы составили за 2 месяца 25000 руб.

*Задание 2*

Внедрение информационной системы, снабженной средствами защиты информации на предприятии, повлекло следующие затраты:

1. Капитальные затраты на внедрение ПС включили:

- затраты на приобретение ПС – 23000 руб.,
- приобретение ЭВМ и периферийного оборудования – 120100 руб.,
- монтаж средств ВТ – 6200 руб.,
- адаптацию ПС - 7000 руб.

В результате реконструкции старой системы было реализовано ВТ и оборудования на сумму 7000 руб.

2. Капитальные затраты на аппаратные средства защиты включили

а) затраты по проектированию системы аппаратной защиты информации сторонней организацией – 82000 руб.

б) затраты на приобретение технических средств – 230000 руб. и монтаж – 50000 руб.

3 Затраты на эксплуатацию системы 3 года включают:

- амортизацию ВТ и ПС;
- зарплата персонала ВЦ и служб защиты – 43000 руб. в мес.;
- текущий ремонт 1800 руб. в мес.;
- оборотные средства – 15000 руб. в год.

Эксплуатации затраты увеличиваются в среднем на 5% в год

Внедрение системы приведет к получению прибыли в размере 2 000 000 в год. Предполагается, что прибыль на второй год эксплуатации возрастет на 5, а на третий - на 10 %. По-экспертным оценки риск финансовых потерь из- за возможные утечки информации может составить- 400 000 руб. в год.

Определить чистый дисконтированный доход и индекс доходности проекта , если норма дисконта составляет 5% на капитал.