

**Министерство науки и высшего образования РФ  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Национальный исследовательский университет «МЭИ»**

**Направление подготовки/специальность: 10.03.01 Информационная безопасность**

**Наименование образовательной программы: Безопасность компьютерных систем**

**Уровень образования: высшее образование - бакалавриат**

**Форма обучения: Очная**

**Оценочные материалы  
по дисциплине  
Организация и управление службой защиты информации**

**Москва  
2022**

## ОЦЕНОЧНЫЕ МАТЕРИАЛЫ РАЗРАБОТАЛ:

Преподаватель

(должность)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Васильев А.С.
	Идентификатор	Re612482f-VasilyevAS-42f74b66

(подпись)

А.С.

Васильев

(расшифровка  
подписи)

## СОГЛАСОВАНО:

Руководитель  
образовательной  
программы

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Баронов О.Р.
	Идентификатор	R90d76356-BaronovOR-7bf8fd7e

(подпись)

О.Р. Баронов

(расшифровка  
подписи)

Заведующий  
выпускающей кафедры

(должность, ученая степень, ученое  
звание)

	Подписано электронной подписью ФГБОУ ВО «НИУ «МЭИ»	
	Сведения о владельце ЦЭП МЭИ	
	Владелец	Невский А.Ю.
	Идентификатор	R4bc65573-NevskyAY-0b6e493d

(подпись)

А.Ю.

Невский

(расшифровка  
подписи)

## ОБЩАЯ ЧАСТЬ

Оценочные материалы по дисциплине предназначены для оценки: достижения обучающимися запланированных результатов обучения по дисциплине, этапа формирования запланированных компетенций и уровня освоения дисциплины.

Оценочные материалы по дисциплине включают оценочные средства для проведения мероприятий текущего контроля успеваемости и промежуточной аттестации.

Формируемые у обучающегося компетенции:

1. ПК-4 способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты
2. ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации
3. ПК-14 способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности

и включает:

**для текущего контроля успеваемости:**

Форма реализации: Письменная работа

1. Инструкции СБП (Проверочная работа)
2. Структура СБП (Проверочная работа)
3. Угрозы и безопасность (Проверочная работа)
4. Управление СБП (Проверочная работа)

## БРС дисциплины

7 семестр

Раздел дисциплины	Веса контрольных мероприятий, %				
	Индекс КМ:	КМ-1	КМ-2	КМ-3	КМ-4
	Срок КМ:	4	8	12	15
Основы организации информационной безопасности организации					
Вводная лекция	+				
Тема 1. Основы организации информационной безопасности организации	+				
Тема 2. Основы организации службы информационной безопасности организации		+			
Тема 3. Порядок разработки нормативных документов для службы информационной безопасности организации		+			

Тема 4. Положение о службе информационной безопасности организации и инструкции должностных лиц службы			+	
Основы управления службой информационной безопасности организации (предприятия)				
Тема 5. Организационная структура управления службой информационной безопасности организации			+	
Тема 6. Особенности организации управления службой информационной безопасности в организациях различных форм собственности				+
Тема 7. Система управления персоналом службы информационной безопасности				+
Тема 8. Основы работы с персоналом службы информационной безопасности				+
Вес КМ:	25	25	25	25

\$Общая часть/Для промежуточной аттестации\$

## СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

### *I. Оценочные средства для оценки запланированных результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций*

Индекс компетенции	Индикатор	Запланированные результаты обучения по дисциплине	Контрольная точка
ПК-4	ПК-4(Компетенция)	Знать: назначение, роль, задачи, функции и виды организационных структур службы информационной безопасности порядок и технологию создания и реорганизации службы информационной безопасности, а также основные методы и технологию управления службой информационной безопасности	Угрозы и безопасность (Проверочная работа) Инструкции СБП (Проверочная работа)
ПК-13	ПК-13(Компетенция)	Знать: основные методы и технологию управления службой информационной безопасности Уметь: определять структуру службы, осуществлять подбор, расстановку и организацию работы должностных лиц службы	Управление СБП (Проверочная работа)

		информационной безопасности	
ПК-14	ПК-14(Компетенция)	Уметь: осуществлять управление и контроль за деятельностью службы информационной безопасности организации (предприятия) и соблюдения режима защиты информации в структурных подразделениях организации (предприятия) организовывать все виды работ службы информационной безопасности	Структура СБП (Проверочная работа)

## II. Содержание оценочных средств. Шкала и критерии оценивания

### КМ-1. Угрозы и безопасность

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Проверочная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** практическая работа

#### Краткое содержание задания:

Взаимодействие и координация. Предполагает осуществление мер обеспечения безопасности на основе четкого взаимодействия всех заинтересованных подразделений и служб, сторонних специализированных организаций в этой области, координацию их усилий для достижения поставленных целей. 10. Совершенствование. Предусматривает совершенствование мер и средств защиты на основе собственного опыта, появления новых 19 Глава 1 технических средств с учетом изменений в методах и средствах разведки и промышленного шпионажа, нормативно-технических требований, накопленного отечественного и зарубежного опыта. 11. Централизация управления. Предполагает самостоятельное функционирование системы безопасности по единым организационным, функциональным и методологическим принципам с централизованным управлением деятельностью системы безопасности. Особое внимание необходимо уделять принципу комплексности. Для обеспечения безопасности во всем многообразии структурных элементов предприятия, при множестве угроз и способов несанкционированного доступа должны применяться все виды и формы защиты и противодействия в полном объеме. Недопустимо применять отдельные формы или технические средства.

#### Контрольные вопросы/задания:

Знать: назначение, роль, задачи, функции и виды организационных структур службы информационной безопасности	1. Назовите основные виды угроз безопасности предприятия 2. Перечислите цель и задачи системы безопасности предприятия. 3. Какие средства используются для обеспечения безопасности предприятия?
---	--

#### Описание шкалы оценивания:

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*

*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

## КМ-2. Инструкции СБП

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Проверочная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** письменная работа

### Краткое содержание задания:

Наиболее важным документом, регламентирующим деятельность службы безопасности предприятия, является закон РФ «О частной детективной и охранной деятельности в РФ». Этим законом регламентируется, что учредителями службы безопасности не могут быть физические лица, даже имеющие соответствующие лицензии. В соответствии с законом учредителем службы безопасности может быть только одно предприятие. В законе четко определено, что служба безопасности создается в интересах собственной безопасности учредителя, однако роль службы безопасности в ее обеспечении не определена. Представляется, что служба безопасности предназначена прежде всего для организации защиты от всех видов угроз. Детализация различных угроз, устранение, пресечение или их нейтрализация входит в компетенцию службы безопасности, должна быть отражена в ее уставе применительно к основным видам безопасности. Приведем краткий перечень возможных действий службы безопасности по пресечению, устранению или нейтрализации угроз в рамках основных видов безопасности [7]. 1. Физическая безопасность – охрана персонала от насильственных преступлений, предупреждение таких преступлений и т.д. 2. Информационная безопасность – сохранение коммерческой тайны, борьба с хакерами и т.д. 3. Экономическая безопасность – охрана имущества предприятия, борьба с экономическим шпионажем и т.д. 4. Экологическая безопасность – документирование экологических правонарушений, выставление экологических постов и т.д. 5. Пожарная безопасность – проектирование, монтаж и эксплуатационное обслуживание пожарной сигнализации, выставление постов в местах загорания и пожаров и т.д. 6. Техногенная безопасность – охрана наиболее опасных участков предприятия от террористов, участие в расследовании техногенных катастроф и т.д. 7. Психологическая безопасность – информирование персонала предприятия об отсутствии реальных угроз, адекватное реагирование на дезинформационные мероприятия и т.д. 22 Правовые основы деятельности службы безопасности предприятия 8. Научно-техническая безопасность – охрана ноу-хау, организация охраны научных лабораторий и т.д.

### Контрольные вопросы/задания:

Знать: порядок и технологию создания и реорганизации службы информационной безопасности, а также основные методы и технологию управления службой информационной безопасности	1. Какими инструкциями руководствуются при организации работы службы безопасности предприятия? 2. Назвать основные виды безопасности на предприятии. 3. Что необходимо включать в коллективный договор для правового обеспечения защиты информации?
--	---

### Описание шкалы оценивания:

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания: Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно*

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*



*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 50

*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

### **КМ-3. Управление СБП**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Проверочная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** проверочная работа

#### **Краткое содержание задания:**

Система управления СБП может быть рассмотрена с позиции общего подхода к построению социальных организационных систем. В этом случае выделяется три вида управленческой деятельности: 1. Стратегическое управление – анализ и прогноз динамики внешней и внутренней ситуации на предприятии, определение целей организационных структур службы безопасности, выявление проблем на пути достижения основной цели; разработка возможных вариантов поэтапного достижения цели, оценка рисков и экономического обоснования. 2. Текущее (календарное) управление – разработка основных технологий организации систем безопасности предприятия, организация взаимодействия всех подразделений службы безопасности, разработка оперативных планов реализации отдельных этапов выбранного варианта стратегической программы

#### **Контрольные вопросы/задания:**

Знать: основные методы и технологию управления службой информационной безопасности	1. Дайте характеристику трех видов управленческой деятельности социальных организационных систем 2. Назначение организационного проектирования (три задачи)
Уметь: определять структуру службы, осуществлять подбор, расстановку и организацию работы должностных лиц службы информационной безопасности	1. В чем состоит суть проектирования организационной структуры системы управления? 2. Какие виды документов разрабатываются при организационном проектировании систем управления? 3. Опишите типовое содержание положения о функциональных структурах подразделения.

#### **Описание шкалы оценивания:**

*Оценка:* 5

*Нижний порог выполнения задания в процентах:* 70

*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка:* 4

*Нижний порог выполнения задания в процентах:* 60

*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 50

*Описание характеристики выполнения знания:* Оценка "удовлетворительно" выставляется если задание преимущественно выполнено

#### **КМ-4. Структура СБП**

**Формы реализации:** Письменная работа

**Тип контрольного мероприятия:** Проверочная работа

**Вес контрольного мероприятия в БРС:** 25

**Процедура проведения контрольного мероприятия:** проверочная работа

#### **Краткое содержание задания:**

Служба безопасности является самостоятельной организационной единицей, подчиняющейся непосредственно руководителю фирмы. Возглавляет службу безопасности начальник службы в должности заместителя руководителя фирмы по безопасности. Структура, численность и состав службы безопасности фирмы определяются реальными финансовыми возможностями, масштабом коммерческой деятельности, степенью конфиденциальности информации. В зависимости от этих факторов служба безопасности может варьировать от двух-трех человек, работающих по совместительству, до полномасштабной службы с развитой структурой (несколько десятков и сотен человек). Наиболее полный состав в виде отделов, групп или отдельных специалистов СБП может включать следующий набор организационных структур: – подразделение охраны; – подразделение режима; – подразделение по работе с кадрами; – подразделение по работе с документами с грифом «Коммерческая тайна» (специальный отдел); – подразделение инженерно-технической защиты; – подразделение разведки; – подразделение контрразведки;

#### **Контрольные вопросы/задания:**

Уметь: организовывать все виды работ службы информационной безопасности	1. По каким направлениям производится расследование факта разглашения коммерческой тайны? 2. Перечислите задачи, выполняемые советом по безопасности предприятия.
Уметь: осуществлять управление и контроль за деятельностью службы информационной безопасности организации (предприятия) и соблюдения режима защиты информации в структурных подразделениях организации (предприятия)	1. Чем определяется состав СБП?

#### **Описание шкалы оценивания:**

*Оценка: 5*

*Нижний порог выполнения задания в процентах: 70*

*Описание характеристики выполнения знания:* Оценка "отлично" выставляется если задание выполнено в полном объеме или выполнено преимущественно верно

*Оценка: 4*

*Нижний порог выполнения задания в процентах: 60*

*Описание характеристики выполнения знания:* Оценка "хорошо" выставляется если большинство вопросов раскрыто. выбрано верное направление для решения задач

*Оценка: 3*

*Нижний порог выполнения задания в процентах: 50*  
*Описание характеристики выполнения знания: Оценка "удовлетворительно" выставляется  
если задание преимущественно выполнено*

# СОДЕРЖАНИЕ ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7 семестр

**Форма промежуточной аттестации:** Зачет с оценкой

**Пример билета**

1. Назовите основные задачи подразделения и охраны. 2. Какие требования предусматривает внутриобъектовый режим?
2. Какие требования предусматривает пропускной режим на предприятии?

**Процедура проведения**

письменный опрос по билетам

***1. Перечень компетенций/индикаторов и контрольных вопросов проверки результатов освоения дисциплины***

**1. Компетенция/Индикатор:** ПК-4(Компетенция)

**Вопросы, задания**

1. Что должен выполнять сотрудник СЗИ?
2. Какие функции рассматриваются при управлении СБП?
3. В чем выражается прогнозирование ситуации со стороны сотрудников СБП?

**Материалы для проверки остаточных знаний**

1. Опасности

Верный ответ: Опасности – это возможные или реальные явления, события и процессы, способные нанести моральный или материальный ущерб предприятию и предпринимательской деятельности.

2. С учетом этого угрозы могут быть классифицированы по следующим признакам

Верный ответ: по величине принесенного ущерба: – предельный, после которого фирма может стать банкротом; – значительный, но не приводящий к банкротству; – незначительный, который фирма за какое-то время может компенсировать и др.; • по вероятности возникновения: – весьма вероятная угроза; – вероятная угроза; – маловероятная угроза; • по причинам появления: – стихийные бедствия; – преднамеренные действия; • по характеру нанесенного ущерба: – материальный; – моральный; • по характеру воздействия: – активные; – пассивные; • по отношению к объекту: – внутренние; – внешние.

3. Законность

Верный ответ: Законность. Предполагает разработку системы безопасности на основе федерального законодательства в области предпринимательской деятельности, информатизации и защиты информации, частной охранной деятельности, а также других нормативных актов по безопасности с применением всех дозволенных методов обнаружения и пресечения правонарушений.

**2. Компетенция/Индикатор:** ПК-13(Компетенция)

**Вопросы, задания**

1. Какие функции возлагаются на специальный отдел?
2. Кто должен входить в состав СЗИ?
3. Назовите перечень основных организационных технических мероприятий, выполняемых сотрудниками СЗИ.

### **Материалы для проверки остаточных знаний**

1. Информационная безопасность (ИБ) – это  
Верный ответ: Информационная безопасность (ИБ) – это состояние защищенности информационной среды предприятия, обеспечивающее его функционирование и развитие в интересах его персонала.
2. Объектом угроз информационной безопасности выступают  
Верный ответ: Объектом угроз информационной безопасности выступают сведения о составе, состоянии и деятельности объекта защиты (персонала, материальных и финансовых ценностей, информационных ресурсов). Угрозы информации выражаются в нарушении ее целостности, конфиденциальности, полноты и доступности.
3. Источниками угроз выступают  
Верный ответ: Источниками угроз выступают конкуренты, преступники, коррупционеры, административно-управленческие органы

### **3. Компетенция/Индикатор: ПК-14(Компетенция)**

#### **Вопросы, задания**

1. Назовите основные принципы организации режима охраны
2. Перечислите виды охранной деятельности.
3. Какие требования предусматривает пропускной режим на предприятии?
4. Перечислите виды деятельности, выполняемые службой информационной безопасности (СЗИ).

### **Материалы для проверки остаточных знаний**

1. Для достижения указанных целей и задач используются различные средства обеспечения безопасности предприятия, среди которых можно выделить следующие  
Верный ответ: • Технические средства. К ним относятся охранно-пожарные системы, видео-радиоаппаратура, средства обнаружения взрывных устройств, бронежилеты, заграждения и т.д. • Организационные средства. Создание специализированных оргструктурных формирований, обеспечивающих безопасность предприятия. • Информационные средства. Прежде всего это печатная и видеопродукция по вопросам сохранения конфиденциальной информации. Кроме этого, важная информация для принятия решений по вопросам безопасности сохраняется в компьютерах. • Финансовые средства. Совершенно очевидно, что без достаточных финансовых средств невозможно функционирование системы безопасности, вопрос лишь в том, чтобы использовать их целенаправленно и с высокой отдачей
2. Разглашение – это  
Верный ответ: Разглашение – это умышленные или неосторожные действия с конфиденциальными сведениями, приведшие к ознакомлению с ними лиц, не допущенных к ним
3. Утечка – это  
Верный ответ: Утечка – это неконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена
4. Несанкционированный доступ  
Верный ответ: Несанкционированный доступ – это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым секретам

## **II. Описание шкалы оценивания**

Оценка: 5

Нижний порог выполнения задания в процентах: 70

*Описание характеристики выполнения знания:* Работа выполнена в рамках "продвинутого" уровня. Ответы даны верно, четко сформулированные особенности практических решений

*Оценка:* 4

*Нижний порог выполнения задания в процентах:* 60

*Описание характеристики выполнения знания:* Работа выполнена в рамках "базового" уровня. Большинство ответов даны верно. В части материала есть незначительные недостатки

*Оценка:* 3

*Нижний порог выполнения задания в процентах:* 50

*Описание характеристики выполнения знания:* Работа выполнена в рамках "порогового" уровня. Основная часть задания выполнена верно. на вопросы углубленного уровня

### ***III. Правила выставления итоговой оценки по курсу***