МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Фонды оценочных средств по дисциплине «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ БИЗНЕСА»

Индикаторы (детализация) компетенции

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

2. Планируемые результаты обучения

Коды индикаторов компетенций	Планируемый результат
ПК.2.1	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

3. Спецификация теста

Тест по дисциплине «Управление информационной безопасностью бизнеса» представляет собой перечень примерных вопросов, предлагаемых студентам с учетом тем и заданий для контрольных мероприятий, предусмотренных по дисциплине.

В тесте *может быть несколько правильных ответов.*

Вариант №1

1 Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности -
а) Сотрудники
б)Хакеры
в) Атакующие
г) Контрагенты (лица, работающие по договору)

2. При анализе стоимости защитных мер следует учитывать:
а) расходы на закупку оборудования
б) расходы на закупку программ
в) расходы на обучение персонала
г) анализ активов

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?
а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
а) Владельцы данных
б) Пользователи
в) Администраторы
г) Руководство организации

6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
а) Поддержка высшего руководства
б) Эффективные защитные меры и методы их внедрения
в) Актуальные и адекватные политики и процедуры безопасности
г) Проведение тренингов по безопасности для всех сотрудников

7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда риски не могут быть приняты во внимание по политическим соображениям
в) Когда необходимые защитные меры слишком сложны
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

8. Что такое политики безопасности?
а) Пошаговые инструкции по выполнению задач безопасности
б) Общие руководящие требования по достижению определенного уровня безопасности
в) Широкие, высокоуровневые заявления руководства
г) Детализированные документы по обработке инцидентов безопасности

9. Эффективная программа безопасности требует сбалансированного применения:
а) Технических и нетехнических методов
б) Контрмер и защитных механизмов
в) Физической безопасности и технических средств защиты
г) Процедур безопасности и шифрования

10. Что из перечисленного не является целью проведения анализа рисков?
а) Делегирование полномочий
б) Количественная оценка воздействия потенциальных угроз
в) Выявление рисков
г) Определение баланса между воздействием риска и стоимостью необходимых контрмер

11. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
а) Поддержка
б) Выполнение анализа рисков
в) Определение цели и границ
г) Делегирование полномочий

12.Что такое стандарт CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
а) Список стандартов, процедур и политик для разработки программы безопасности
б) Текущая версия ISO 17799
в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
г) Открытый стандарт, определяющий цели контроля

13. Из каких четырех доменов состоит стандарт CobiT?
а) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
б) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
в) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
г) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

14. Что представляет собой стандарт ISO/IEC 27799?
а) Стандарт по защите персональных данных о здоровье
б) Новая версия BS 17799
в) Определения для новой серии ISO 27000
г) Новая версия NIST 800-60

15. Защита информации это:
а) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
б) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;
в) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;
г) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям.

16. Стандарты СУИБ:
а) ISO/IEC 17799;
б) ГОСТ Р ИСО/МЭК 27001-2006;
в) BS 25999;
г) ГОСТ Р ИСО/МЭК 18045-2013.

17. Стандарт PCI DSS
а) стандарт безопасности данных индустрии платёжных карт;
б) стандарт СУИБ;
в) стандарт разработки политики безопасности информации;
г) стандарт мер защиты в организации.

18. Управление рисками ИБ предполагает
а) установление контекста управления рисками ИБ;
б) оценку, обработку и принятие рисков ИБ;
г) мониторинг, пересмотр рисков ИБ;
д) коммуникацию рисков ИБ.

19. Обработка рисков ИБ это:
а) процесс изменения риска ИБ;
б) процесс выбора и реализации мер по изменению риска ИБ ;
в) процесс выбора и осуществления защитных мер, снижающих риски ИБ, или мер по переносу, принятию или уходу от рисков ИБ ;
г) процесс выбора и осуществления мер по модификации (изменению) рисков ИБ.

20. Стандарты ЦБ РФ в области СМИБ
а) СТО БР ИББС-1.0-2014
б) СТО БР ИББС-1.1-2007
в) СТО БР ИББС-1.2-2014
г) СТО БР ИББС-1.8-2019

Вариант №2

1. СУИБ включает
а) организационную структуру,
б) политику ИБ,
в) обязанности персонала,
г) ресурсы в области ИБ.

2. Информационная безопасность организации.
а) Состояние защищенности интересов организации в условиях угроз в информационной сфере.
б) Установка средств защиты в АС организации;
в) Процесс оценки и обработки рисков ИБ в организации;
г) Выполнение норм и правил утвержденных руководством.

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?
а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
в) Улучшить контроль за безопасностью этой информации
г) Снизить уровень классификации этой информации

4. Что самое главное должно продумать руководство при классификации данных?
а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
б) Необходимый уровень доступности, целостности и конфиденциальности
в) Оценить уровень риска и отменить контрмеры
г) Управление доступом, которое должно защищать данные

5. Разработка и внедрение СУИБ предполагает
а) Оценку рисков ИБ
б) Разработку и утверждение политики ИБ
в) Обработку рисков
г) Обеспечение непрерывности бизнеса

6. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
а) Поддержка высшего руководства
б) Эффективные защитные меры и методы их внедрения
в) Актуальные и адекватные политики и процедуры безопасности
г) Проведение тренингов по безопасности для всех сотрудников

7. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда риски не могут быть приняты во внимание по политическим соображениям
в) Когда необходимые защитные меры слишком сложны
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери

8. Что такое политика безопасности информации в организации?
а) Пошаговые инструкции по выполнению задач безопасности
б) Совокупность документированных правил, процедур, практических приемов обеспечения ИБ;
в) Руководящие принципы в области безопасности информации, которыми руководствуется организация в своей деятельности;
г) Правила эксплуатации СЗИ.

9. Эффективная программа безопасности требует сбалансированного применения:
а) Технических и нетехнических методов
б) Контрмер и защитных механизмов
в) Физической безопасности и технических средств защиты
г) Процедур безопасности и шифрования

10. Что из перечисленного не является целью проведения анализа рисков?
а) Обработка рисков
б) Количественная оценка воздействия потенциальных угроз
в) Выявление рисков
г) Определение баланса между воздействием риска и стоимостью необходимых контрмер

11. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
а) Поддержка
б) Выполнение анализа рисков
в) Установка СЗИ
г) Делегирование полномочий

12.Что такое стандарт CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
а) Список стандартов, процедур и политик для разработки программы безопасности
б) Текущая версия ISO 17799
в) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
г) Открытый стандарт, определяющий цели контроля

13. Из каких четырех доменов состоит стандарт CobiT?
а) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
б) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
в) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
г) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

14. Стандарт управления инцидентами ИБ
а) ISO/IEC 27035:2011
б) BS 17799
в) ISO 27001
г) NIST 800-60

15. СТО БР ИББС-1.0-2014 состоит разделов:
а) Модели угроз и нарушителей ИБ организаций БС РФ.
б) Система ИБ организации БС РФ.
в) Система менеджмента ИБ организации БС РФ.
г) Проверка и оценка ИБ организаций БС РФ.

16. Стандарты СУИБ:
а) ISO/IEC 17799;
б) ГОСТ Р ИСО/МЭК 27001-2006;
в) ISO/IEC 9001;
г) ГОСТ Р ИСО/МЭК 18045-2013.

17. Стандарт PCI DSS
а) стандарт безопасности данных индустрии платёжных карт;
б) стандарт СУИБ;
в) стандарт разработки политики безопасности информации;
г) стандарт мер защиты в организации.

18. Управление рисками ИБ предполагает
а) установление контекста управления рисками ИБ;
б) оценку, обработку и принятие рисков ИБ;
в) аудит рисков ИБ;
г) коммуникацию рисков ИБ.

19. Обработка рисков ИБ это:
а) процесс измерения риска ИБ;
б) процесс выбора и реализации мер по изменению риска ИБ ;
в) процесс выбора и осуществления защитных мер, снижающих риски ИБ, или мер по переносу, принятию или уходу от рисков ИБ ;
г) процесс выбора и осуществления мер по модификации (изменению) рисков ИБ.

20. Действующие стандарты ЦБ РФ в области СМИБ
а) СТО БР ИББС-1.0-2014
б) СТО БР ИББС-1.0-2007
в) СТО БР ИББС-1.1-2007
г) СТО БР ИББС-1.3-2019

Ключ к тесту

Вариант 1	Вариант 2
1 а	1 а,б,в,г
2 а,б,в,г	2 а
3 в	3 в
4 б	4 б
5 г	5 а,б,в
6 а	6 а
7 г	7 г
8 в	8 б,в
9 а	9 а
10 а	10 а
11 б	11 а,г
12 г	12 г
13 а	13 а
14 а	14 а
15 г	15 а,б,в,г
16 а,б,в,г	16 а,б, г
17 а	17 а
18 а,б,в,г	18 а,б,г
19 а,б,в,г	19 б,в,г
20 а,б,в	20 а,в