Государственное образовательное учреждение
«Приднестровский государственный университет им. Т.Г. Шевченко»

Физико-технический институт

Факультет информатики и вычислительной

Кафедра программного обеспечения вычислительной техники

УТВЕРЖДАЮ

Заведующий кафедрой ПОВТ


С.Г. Федорченко

«28» августа 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

ОСНОВЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Направление подготовки
09.04.02 Информационные системы и технологии

Профиль подготовки
Защита информации в информационных системах

Квалификация (степень) выпускника:	**магистр**
Форма обучения:	**очная, заочная**
Год набора:	**2023 г.**

Разработал:
к.п.н., доцент кафедры ПОВТ,


/С.В. Помян

«28» августа 2024 г.

Тирасполь, 2024

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Основы управления информационной безопасностью» у обучающегося должны быть сформированы следующие компетенции:

Категория общепрофессиональных компетенций	Код и наименование общепрофессиональной компетенции	Код и наименование индикатора достижения общепрофессиональной компетенции
Общепрофессиональные компетенции выпускников и индикаторы их достижения		
-	ОПК-3. Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ИД-1$_{ОПК-3}$ Знать принципы, методы и средства анализа и структурирования профессиональной информации
		ИД-2$_{ОПК-3}$ Уметь анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров
		ИД-3$_{ОПК-3}$ Иметь навыки: подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями

2. Программа оценивания контролируемой компетенции:

Текущая аттестация	Контролируемые модули, разделы (темы) дисциплины их название	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
РУБЕЖНЫЙ КОНТРОЛЬ	Раздел 1 Введение в основы управления информационной безопасностью Раздел 2 Системы управления ИБ	ОПК-3	Презентация Кейс-задача №1
РУБЕЖНАЯ АТТЕСТАЦИЯ	Раздел 3 Основы управления рисками ИБ Раздел 4 Процессы управления ИБ		Кейс-задача №2 Кейс-задача №3 Итоговый тест
Промежуточная аттестация		Код контролируемой компетенции (или ее части)	Наименование оценочного средства
№1		ОПК-3	Зачет

3. Показатели и критерии оценивания компетенции по этапам формирования, описание шкал оценивания

Этапы оценивания компетенции	Показатели достижения заданного уровня освоения компетенции	Критерии оценивания результатов обучения			
		2	**3**	**4**	**5**
Первый этап	ИД-1$_{ОПК-3}$ Знать принципы, методы и средства анализа и структурирования профессиональной информации	Не знает	Знает принципы, методы и средства анализа	Знает принципы, методы и средства анализа и структурирования	Знает принципы, методы и средства анализа и структурирования профессиональной информации
Второй этап	ИД-2$_{ОПК-3}$ Уметь анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров	Не умеет	Умеет анализировать профессиональную информацию	Умеет анализировать профессиональную информацию, выделять в ней главное	Умеет анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров
Третий этап	ИД-3$_{ОПК-3}$ Иметь навыки: подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями	Не владеет	Имеет навыки подготовки научных докладов	Иметь навыки подготовки научных докладов, публикаций и аналитических обзоров	Иметь навыки: подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами и рекомендациями

4. Шкала оценивания

Согласно Положению «О порядке организации аттестации в ИТИ ПГУ им. Т.Г. Шевченко, итоговая оценка представляет собой сумму баллов, полученных студентом по итогу освоения дисциплины (модуля):

Оценка в традиционной шкале	Оценка в 100-балльной шкале	Буквенные эквиваленты оценок в шкале ЗЕ (% успешно аттестованных)
5 (отлично)	88–100	A (отлично) – 88-100 баллов
4 (хорошо)	70–87	B (очень хорошо) – 80-87баллов
		C (хорошо) – 70-79 баллов
3 (удовлетворительно)	50–69	D (удовлетворительно) – 60-69 баллов
		E (посредственно) – 50-59 баллов
2 (неудовлетворительно)	0–49	Fx – неудовлетворительно, с возможной пересдачей – 21-49 баллов
		F – неудовлетворительно, с повторным изучением дисциплины – 0-20 баллов

Расшифровка уровня знаний, соответствующего полученным баллам, дается в таблице, указанной ниже

A	“Отлично” - теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному.
B	“Очень хорошо” - теоретическое содержание курса освоено полностью, без пробелов, необходимые практические навыки работы с освоенным материалом в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество выполнения большинства из них оценено числом баллов, близким к максимальному.
C	“Хорошо” - теоретическое содержание курса освоено полностью, без пробелов, некоторые практические навыки работы с освоенным материалом сформированы недостаточно, все предусмотренные программой обучения учебные задания выполнены, качество выполнения ни одного из них не оценено минимальным числом баллов, некоторые виды заданий выполнены с ошибками.
D	“Удовлетворительно” - теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, необходимые практические навыки работы с освоенным материалом в основном сформированы, большинство предусмотренных программой обучения учебных заданий выполнено, некоторые из выполненных заданий, возможно, содержат ошибки.
E	“Посредственно” - теоретическое содержание курса освоено частично, некоторые практические навыки работы не сформированы, многие предусмотренные программой обучения учебные задания не выполнены, либо качество выполнения некоторых из них оценено числом баллов, близким к минимальному.
FX	“Условно неудовлетворительно” - теоретическое содержание курса освоено частично, необходимые практические навыки работы не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, либо качество их выполнения оценено числом баллов, близким к минимальному; при дополнительной самостоятельной работе над материалом курса возможно повышение качества выполнения учебных заданий.
F	“Безусловно неудовлетворительно” - теоретическое содержание курса не освоено, необходимые практические навыки работы не сформированы, все выполненные учебные задания содержат грубые ошибки, дополнительная самостоятельная работа над материалом курса не приведет к какому-либо значимому повышению качества выполнения учебных заданий.

5. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций при изучении учебной дисциплины в процессе освоения образовательной программы

5.1 Типовой вариант тематик Презентация П1

1. Стандартизация в области управления ИБ
2. Системы управления информационной безопасностью
3. Процессный подход
4. Область деятельности СУИБ.
5. Ролевая структура СУИБ. Политика СУИБ
6. Основы управления рисками ИБ
7. Рискология ИБ
8. Анализ рисков ИБ
9. Процессы управления ИБ
10. Основные процессы СУИБ.
11. Обязательная документация СУИБ
12. Внедрение разработанных процессов
13. Управление инцидентами ИБ.
14. Эксплуатация и независимый аудит СУИБ

15. Документные системы ИБ
Минимальное количество слайдов – 10, к каждому слайду должен быть предоставлен доклад, сопровождающий презентацию.
Максимальное количество баллов – 20. Соответствие содержания теме – 4 балла, качество графической информации, дизайн – 2 балла, подбор информации для создания слайда – 4 балла, личный вклад автора – 4 балла, грамотность и логичность изложения материала – 2 бала, соответствие оформления стандартам – 2 балла, своевременность сдачи – 2 балла.

5.2 Типовой вариант Кейс-задача №1.

Задание: разработать две частные политики ИБ на ваш выбор (см. ПЗ 9-10,11-12 Основы управления ИБ часть 4) Организация/Учреждение/Компания.
Организация/Учреждение/Компания – это может быть Организация/Учреждение/Компания, в которой вы работаете, или любая абстрактная.
Разработанная высокоуровневая политика ИБ для выбранной вами Организации/Учреждения/Компании должна быть адаптированной к этой Организации/Учреждению/Компании.
Максимальное количество баллов – 20. Соответствие содержания теме – 4 балла, качество информации,– 2 балла, подбор информации– 4 балла, личный вклад автора – 4 балла, грамотность и логичность изложения материала – 2 бала, соответствие оформления стандартам – 2 балла, своевременность сдачи – 2 балла.

5.4 Типовой вариант: Кейс-задача №2.

*Задание**:*** разработать *любое положение/перечень/инструкцию* из перечисленных в примере ниже:
- положение о сохранении конфиденциальной информации;
- перечень сведений, которые составляют конфиденциальную информацию;
- инструкция о порядке допуска сотрудников к сведениям, которые составляют конфиденциальную информацию;
- положение о специальном делопроизводстве и документообороте;
- перечень сведений, которые разрешены к опубликованию в открытой печати;
- положение о работе с иностранными фирмами и их представителями;
- обязательство сотрудника о сохранении конфиденциальной информации;
- памятка сотруднику о сохранении коммерческой тайны.

Максимальное количество баллов – 20. Соответствие содержания теме – 4 балла, качество информации,– 2 балла, подбор информации– 4 балла, личный вклад автора – 4 балла, грамотность и логичность изложения материала – 2 бала, соответствие оформления стандартам – 2 балла, своевременность сдачи – 2 балла.

5.5 Типовой вариант: Кейс-задача №3.

Задание: разработать часть СУИБ любой Организации/Учреждения/Компании на ваш выбор, которая должна включать:
1) высокоуровневую политику ИБ);
2) две частные политики ИБ на ваш выбор
3) любое положение/перечень/инструкцию.

Организация/Учреждение/Компания – это может быть Организация/Учреждение/Компания, в которой вы работаете, или любая абстрактная.
Разработанная высокоуровневая политика ИБ для выбранной вами Организации/Учреждения/Компании должна быть адаптированной к этой Организации/Учреждению/Компании.

Пример высокоуровневой политики информационной безопасности:
Политика информационной безопасности.
Настоящая политика определяет цели и принципы обеспечения информационной безопасности в Компании.
Политика распространяется на главный офис Компании и все филиалы. Политика обязательна для исполнения всеми сотрудниками, а также лицами, работающими с информацией, принадлежащей Компании, в рамках заключенных контрактов.
Под обеспечением информационной безопасности или защитой информации понимается сохранение ее конфиденциальности, целостности и доступности. Конфиденциальность информации обеспечивается в случае предоставления доступа к данным только авторизованным лицам, целостность в случае внесения в данные исключительно авторизованных изменений, доступность при обеспечении возможности получения доступа к данным авторизованным лицам в нужное для них время.
Целями обеспечения информационной безопасности являются минимизация ущерба от реализации угроз информационной безопасности и улучшение деловой репутации и корпоративной культуры Компании.
Информация является важным активом Компании и ее защита является обязанностью каждого сотрудника.
Доступ к информации предоставляется только лицам, которым он необходим для выполнения должностных или контрактных обязательств в минимально возможном объеме.
Для каждого информационного ресурса определяется владелец, отвечающий за предоставление к нему доступа и эффективное функционирование мер защиты информации.
Сотрудники Компании проходят регулярное обучение в области информационной безопасности.
В Компании ежегодно проводится независимый аудит информационной безопасности.
Генеральный директор Компании утверждает политики информационной безопасности.
Отдел информационной безопасности отвечает за определение детальных требований информационной безопасности и контролирует их исполнение в Компании.
Система управления информационной безопасностью в Компании строится на основе международных стандартов ISO 27001 и ISO 27002.
Меры защиты информации внедряются по результатам проведения оценки рисков информационной безопасности.
Оценка рисков информационной безопасности проводится ежегодно, а также в случае значительных изменений в структуре Компании и ее бизнес-процессах.
При оценке рисков учитывается влияние реализации угроз информационной безопасности на финансовое положение Компании и ее репутацию на рынке.
Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз.
Успешное достижение целей настоящей политики возможно только при выполнении положений следующих частных (детальных) политик информационной безопасности:
Политика использования паролей;

Политика использования сети Интернет;
Политика использования электронной почты;
…
Несоблюдение политик информационной безопасности сотрудниками Компании может повлечь дисциплинарные меры взыскания вплоть до увольнения.
Кроме политики и программы информационной безопасности на предприятии разрабатываются следующие документы:

- положение о сохранении конфиденциальной информации;
- перечень сведений, которые составляют конфиденциальную информацию;
- инструкция о порядке допуска сотрудников к сведениям, которые составляют конфиденциальную информацию;
- положение о специальном делопроизводстве и документообороте;
- перечень сведений, которые разрешены к опубликованию в открытой печати;
- положение о работе с иностранными фирмами и их представителями;
- обязательство сотрудника о сохранении конфиденциальной информации;
- памятка сотруднику о сохранении коммерческой тайны.

Максимальное количество баллов – 20. Соответствие содержания теме – 4 балла, качество информации,– 2 балла, подбор информации– 4 балла, личный вклад автора – 4 балла, грамотность и логичность изложения материала – 2 бала, соответствие оформления стандартам – 2 балла, своевременность сдачи – 2 балла.

5.5 Типовой вариант итогового теста

1. Кто является основным ответственным за определение уровня классификации информации

а) Руководитель среднего звена
б) Высшее руководство
в) Владелец
г) Пользователь

2. 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)

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

6. Что такое процедура

а) Правила использования программного и аппаратного обеспечения в компании

б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

7. 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

8. 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

9. 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

10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер

а) Анализ рисков

б) Анализ затрат / выгоды

в) Результаты ALE

г) Выявление уязвимостей и угроз, являющихся причиной риска

11. Что лучше всего описывает цель расчета ALE

а) Количественно оценить уровень безопасности среды

б) Оценить возможные потери для каждой контрмеры

в) Количественно оценить затраты / выгоды

г) Оценить потенциальные потери от угрозы в год

12. Тактическое планирование – это:

а) Среднесрочное планирование
б) Долгосрочное планирование
в) Ежедневное планирование
г) Планирование на 6 месяцев

13. Что является определением воздействия (exposure) на безопасность

а) Нечто, приводящее к ущербу от угрозы
б) Любая потенциальная опасность для информации или систем
в) Любой недостаток или отсутствие информационной безопасности
г) Потенциальные потери от угрозы

14. 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

15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:

а) Внедрение управления механизмами безопасности
б) Классификацию данных после внедрения механизмов безопасности
в) Уровень доверия, обеспечиваемый механизмом безопасности
г) Соотношение затрат / выгод

16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации

а) Только военные имеют настоящую безопасность
б) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
в) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

17. Как рассчитать остаточный риск

а) Угрозы х Риски х Ценность актива
б) (Угрозы х Ценность актива х Уязвимости) х Риски
в) SLE х Частоту = ALE
г) (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля

18. 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

19. 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

20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании

а) Чтобы убедиться, что проводится справедливая оценка

б) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ

в) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа

г) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

21. Что является наилучшим описанием количественного анализа рисков

а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности

б) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков

в) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков

г) Метод, основанный на суждениях и интуиции

22. Почему количественный анализ рисков в чистом виде не достижим

а) Он достижим и используется

б) Он присваивает уровни критичности. Их сложно перевести в денежный вид.

в) Это связано с точностью количественных элементов

г) Количественные измерения должны применяться к качественным элементам

23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа

а) Много информации нужно собрать и ввести в программу

б) Руководство должно одобрить создание группы

в) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки

г) Множество людей должно одобрить данные

24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств

а) Стандарты

б) Должный процесс (Due process)

в) Должная забота (Due care)

г) Снижение обязательств

25. Что такое 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

26. Из каких четырех доменов состоит 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

27. 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

28. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO

а) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам

б) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень

в) COSO учитывает корпоративную культуру и разработку политик

г) COSO – это система отказоустойчивости

29. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами

а) NIST и OCTAVE являются корпоративными

б) NIST и OCTAVE ориентирован на ИТ

в) AS/NZS ориентирован на ИТ

г) NIST и AS/NZS являются корпоративными

30. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой

а) Анализ связующего дерева

б) AS/NZS

в) NIST

г) Анализ сбоев и дефектов

Случайным образом выбирается 20 вопросов, каждый правильный ответ – 1 балл, максимальное количество баллов – 20.

5.6 Типовой тест промежуточной аттестации

Вариант 1

1. Команда по разработке политики безопасности обычно включает следующее число человек:

1) от 2 до 5

2) от 2 до 10

3) от 2 до 15

4) от 2 до 20

2. Количество основных правил глобальной политики безопасности равно:

1) трем
2) четырем
3) пяти
4) шести

3. В основные обязанности пользователя данными входит следующее их число:

1) два
2) три
3) четыре
4) пять

4. Какой самый важный вопрос должна решить команда по разработке политики безопасности организации:

1) какие компьютерные и сетевые сервисы требуются для бизнеса
2) зависят ли компьютерные и сетевые сервисы от удаленного доступа к внутренней сети
3) имеется ли требование бизнеса на тот или иной сервис
4) имеются ли требования по доступу к Веб-ресурсам

5. Основные устанавливаемые роли в безопасности сети включают следующее их количество:

1) два
2) три
3) четыре
4) пять

6. Процедура управления конфигурацией определяет:

1) какую информацию следует регистрировать и прослеживать
2) как тестируется и инсталлируется новое аппаратное обеспечение
3) как тестируется и инсталлируется новое программное обеспечение
4) кто должен быть проинформирован, когда вносятся изменения в различные виды обеспечения

7. Первые шаги по разработке политики безопасности включают следующее их число:

1) три
2) четыре
3) пять
4) шесть

8. Процедура реагирования на события определяет:

1) какую информацию следует регистрировать и прослеживать
2) кто имеет полномочия выполнять изменения конфигурации аппаратного и программного обеспечения
3) как обрабатывать исследование отклонений от нормы
4) как следует реагировать на атаки вторжения

9. На этапе анализа рисков осуществляются следующее число действий:

1) три
2) четыре
3) пять
4) шесть

10. При разработке политики ИБ необходимо руководствоваться следующим основным правилом:

1) команда разработчиков политики ИБ не должна превышать 20 человек
2) стоимость защиты конкретного актива не должна превышать стоимости самого актива
3) как следует реагировать на атаки вторжения
4) какую информацию следует регистрировать и прослеживать при функционировании системы защиты

11. Архитектура безопасности включает как минимум следующее число компонентов:

1) два
2) три
3) четыре
4) пять

12. В политике безопасности организации должны быть определены:

1) стандарты
2) правила безопасности
3) операции безопасности
4) процессы безопасности

13. Каждое действие в процессе безопасности включает следующее число компонентов:

1) два
2) три
3) четыре
4) пять

14. Каждое действие в процессе безопасности включает:

1) операцию
2) механизм
3) управление
4) выход

15. Защищаемые ресурсы (данные, файлы, базы данных, программы) могут быть разделены на следующее число групп:

1) два
2) три
3) четыре
4) пять

16. Компоненты архитектуры безопасности включают:

1) физическую безопасность
2) логическую безопасность
3) периметр безопасности сети
4) защиту ресурсов

17. Административные полномочия подразделяются на следующее число категорий:

1) два
2) три
3) четыре
4) пять

18. В основные задачи управления ИБ входят:

1) управление конфигурациями объектов и субъектов доступа;
2) управление доступом к базе данных
3) управление учетными записями и правами доступа к активным сетевым устройствам, рабочим станциям и серверам
4) управление конфигурациями объектов и субъектов доступа

19. Последовательность процессов для обнаружения проблемы и выдачи сигнала тревоги включает следующее число шагов:

1) два
2) три
3) четыре
4) пять

20. Подсистемы управления обновлениями позволяют автоматизировать следующие задачи:

1) возможность назначения обновлений определенным рабочим станциям и серверам или группам рабочих станций и серверов
2) контроль времени обновления ПО
3) автоматическое получение обновлений с сайтов производителей ПО
4) организацию централизованного хранилища обновлений

21. Использование централизованного управления рабочими станциями и серверами позволяет:

1) создавать типовые образы рабочих станций и серверов
2) существенно сократить затраты на обеспечение актуальной конфигурации оборудования
3) распределять административные роли по типам и группам устройств
4) поддерживать соответствие локальных настроек политике безопасности организации

22. Основные задачи управления ИБ включают следующее их число:

1) два
2) три
3) четыре
4) пять

23. Подсистемы управления обновлениями позволяют автоматизировать следующее число задач:

1) два
2) три
3) четыре
4) пять

24. Централизованное управление сетевым оборудованием позволяет:

1) осуществлять мониторинг сетевых устройств
2) производить откат неудачных изменений конфигурации
3) поддерживать соответствие локальных настроек политике безопасности организации
4) централизованно хранить конфигурации активного сетевого оборудования

25. Использование централизованного управления рабочими станциями и серверами позволяет удовлетворить следующее число требований:

1) два
2) три
3) четыре
4) пять

26. В настоящее время наибольшую популярность получили следующие технологии, реализующие модель AAA:

1) RADIUS
2) TACACS
3) RADIUS+
4) TACACS+

27. Централизованное управление сетевым оборудованием позволяет удовлетворить следующее число требований:

1) два
2) три
3) четыре
4) пять

28. GSM в сфере ИБ — это:

1) аналог системы ГЛОНАСС
+2) концепция глобального управления безопасностью
3) узкоспециализированная система централизованного управления безопасностью
4) децентрализованная система управления безопасностью

29. При организации доступа к сетевому оборудованию модель AAA подразумевает выполнение следующего числа процедур:

1) два
2) три
3) четыре
4) пять

30. В GSM, как правило, используется:

1) матричный метод доступа
2) мандатное управление доступом
3) дискреционное управление доступом
4) избирательное управление доступом

Вариант 2

1. Задача ролевого разграничения доступа к конфигурационным командам реализуется инструментальными комплексами в следующее число этапов:

1) два
2) три
3) четыре
4) пять

2. Задача ролевого разграничения доступа к конфигурационным командам реализуется инструментальными комплексами при выполнении следующих этапов:

1) сканирование активного сетевого оборудования
2) анализ полученных результатов и создание политики безопасности с целью разграничения доступа к конфигурационным командам

3) проверки данных учетной записи с целью установки соответствия пользователя множеству зарегистрированных субъектов доступа

4) создание конфигурации для ролевого разграничения доступа командам

3. GSM позволяет построить комплексную систему управления и защиты информационных ресурсов предприятия, обладающую следующим числом основных свойств:

1) 5
2) 6
3) 7
4) 8

4. Группы, на которые могут быть разбиты правила глобальной политики безопасности включают:

1) правила пакетной фильтрации
2) правила VPN
3) правила, отвечающие за мониторинг инцидентов
4) прокси-правила

5. GSM, ориентированная на управление безопасностью предприятия на принципах PBM, удовлетворяет следующему количеству требований:

1) два
2) три
3) четыре
4) пять

6. Правила глобальной политики безопасности могут быть распространены как на:

1) сетевые взаимодействия
2) функции контроля системы
3) функции мониторинга системы
4) функции контроля и управления системы

7. Согласно концепции GSM организация централизованного управления безопасностью КИС основана на следующем числе принципов:

1) два
2) три
3) четыре
4) пять

8. Объектами глобальной политики безопасности могут быть:

1) структурные подразделения компании
2) отдельная фирма
3) подразделение аудита фирмы
4) финансовый департамент

9. Функционально правила глобальной политики безопасности могут быть разбиты на следующее число групп:

1) два
2) три
3) четыре
4) пять

10. В число политик безопасности входят:

1) стартовая политика безопасности устройства
2) политика реагирования на события

3) локальная политика безопасности
4) политика допустимого использования

11. Управление информационными рисками в целях обеспечения ИБ предполагает решение следующего числа основных задач:

1) два
2) четыре
3) шесть
4) восемь

12. При реализации мандатной политики доступа:

1) все субъекты и объекты системы должны быть идентифицированы
2) права доступа субъекта к объекту системы определяются на основании некоторого правила
3) каждому объекту системы присваивается метка критичности
4) каждому субъекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ

13. Реализация методологии оценки рисков ИБ по NIST SP 800-30 включает следующее число основных шагов:

1) 8
2) 9
3) 10
4) 11

14. Управление рисками в сфере ИБ реализуется на следующем уровне:

1) процедурном
2) административном
3) архитектурном
4) мандатном

15. Обязательным условием начала разработки политики ИБ является:

1) наличие на фирме службы защиты информации
2) наличие на фирме функционирующей ИС
3) наличие на фирме высококвалифицированных специалистов в области защиты информации
4) возможность привлечения к разработке политики ИБ сторонних специалистов

16. Основные положения политики безопасности организации описываются в следующем количестве документов:

1) три
2) четыре
3) пять
4) шесть

17. К специализированным политикам, затрагивающим значительное число пользователей, относятся:

1) политика защиты информации
2) политика удаленного доступа к ресурсам сети;
3) политика безопасности виртуальных защищенных сетей
4) политика допустимого использования

18. Преимуществом мандатного метода управления доступом, используемого в соответствующей политике ИБ, является:

1) обеспечение более высокой надежности работы самой ИС

2) простота определения правил разграничения доступа

3) широкое распространение данного метода для работы с конфиденциальной информацией

4) предотвращение утечки информации из объектов с высокой меткой конфиденциальности в объекты с низкой меткой конфиденциальности

19. Варианты реализации стратегии управления рисками включают следующее их число:

1) два

2) три

3) четыре

4) пять

20. Специализированные политики безопасности подразделяются на следующее число групп:

1) две

2) три

3) четыре

4) пять

21. Политика допустимого использования предназначается в основном для:

1) администраторов сети

2) администраторов безопасности

3) конечных пользователей

4) всех вышеуказанных сотрудников

22. К полностью информационным рискам относятся:

1) инвестиционный

2) валютный

+3) управленческий

4) торговый

23. Политика допустимого использования обязательна для:

1) государственных организаций

+2) образовательных учреждений

3) коммерческих фирм

4) всех вышеуказанных организаций

24. Процедуры безопасности описывают:

1) каковы основные правила защиты

2) как защитить ресурсы

3) каковы механизмы исполнения политики ИБ

4) как реализовывать политику ИБ

25. Каждое действие в процессе безопасности включает:

1) операцию

2) механизм

3) управление

4) выход

26. Какой самый важный вопрос должна решить команда по разработке политики безопасности организации:

1) какие компьютерные и сетевые сервисы требуются для бизнеса

2) зависят ли компьютерные и сетевые сервисы от удаленного доступа к внутренней сети

3) имеется ли требование бизнеса на тот или иной сервис

4) имеются ли требования по доступу к Веб-ресурсам

27. Количество основных категорий угроз безопасной передачи данных в вычислительных сетях равно

1) двум

2) трем

3) четырем

4) пяти

28. Новое семейство международных стандартов на системы управления информационной безопасностью имеет код:

1) 17000

2) 27000

3) 37000

4) 47000

29. Одним из последних стандартов серии ISO 27000, принятых до 2014 г., является стандарт:

1) ISO 27011

2) ISO 27023

3) ISO 27032

4) ISO 27799

30. Основное назначение протоколов IPSec заключается в обеспечении:

1) контроля целостности на уровне пакетов данных

2) аутентификации источника данных

3) конфиденциальности передаваемых данных

4) защиты пакетов данных на канальном уровне

5.7 Вопросы к зачету по дисциплине

«**Основы управления информационной безопасностью**»

1. Стандартизация в области управления ИБ
2. Системы управления информационной безопасностью
3. Процессный подход
4. Область деятельности СУИБ.
5. Ролевая структура СУИБ. Политика СУИБ
6. Основы управления рисками ИБ
7. Рискология ИБ
8. Анализ рисков ИБ
9. Процессы управления ИБ
10. Основные процессы СУИБ.
11. Обязательная документация СУИБ
12. Внедрение разработанных процессов
13. Управление инцидентами ИБ.
14. Эксплуатация и независимый аудит СУИБ
15. Документные системы ИБ