Государственное образовательное учреждение
"Приднестровский государственный университет им. Т.Г. Шевченко"

Физико-технический институт

Кафедра информационных технологий

УТВЕРЖДАЮ

Заведующий кафедрой ИТ

Ю.А. Столяренко

«28» августа 2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине
КОРПОРАТИВНАЯ БЕЗОПАСНОСТЬ

Направление подготовки
2.09.03.01 Информатика и вычислительная техника

Профиль подготовки
Вычислительные машины, комплексы, системы и сети

Квалификация (степень) выпускника: **бакалавр**

Форма обучения: **очная, заочная**

Год набора: **2021 г.**

Разработал:
к.т.н., доцент кафедры ИТиАУПП,

/Ю.А. Столяренко

«28» августа 2024 г.

Тирасполь, 2024

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Корпоративная безопасность» 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-1. Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального исследования в профессиональной деятельности	ИД-1$_{ОПК-1}$ Знать основы высшей математики, физики, экологии, инженерной графики, информатики и программирования
		ИД-2$_{ОПК-1}$ Уметь решать стандартные профессиональные задачи с применением естественнонаучных и обще-инженерных знаний, методов математического анализа и моделирования
		ИД-3$_{ОПК-1}$ Владетьметодами теоретического и экспериментального исследования объектов профессиональной деятельности
-	ПК-9. Способен обеспечивать информационную безопасность на уровне БД	ИД-1$_{ПК-9}$ Знать: методы обеспечения информационной безопасности на уровне БД
		ИД-1$_{ПК-9}$ Уметь: анализировать угрозы информационной безопасности на уровне БД
		ИД-1$_{ПК-9}$ Владеть: способами обеспечения информационной безопасности на уровне БД

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. Основные понятия и определения Раздел 2. Принципы защиты информации	ОПК-1, ПК-9	Контрольная работа №1 Лабораторная работа №1 Лабораторная работа №2
РУБЕЖНАЯ АТТЕСТАЦИЯ	Раздел 4. Теоретические аспекты информационной безопасность Раздел 5. Обеспечение информационной безопасность		Контрольная работа №2 Лабораторная работа №3 Лабораторная работа №4 Лабораторная работа №5

Промежуточная аттестация	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
№1	ОПК-1, ПК-9	Экзамен

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$_{УК-1}$ Знать: методики сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа	Не знает	Знает методики сбора и обработки информации	Знает методики сбора и обработки информации; актуальные российские и зарубежные источники информации	Знает методики сбора и обработки информации; актуальные российские и зарубежные источники информации в сфере профессиональной деятельности; метод системного анализа
Второй этап	ИД-2$_{УК-1}$ Уметь: применять методики поиска, сбора и обработки информации: осуществлять критический анализ и синтез информации, полученной из разных источников	Не умеет	Умеет применять методики поиска, сбора и обработки информации	Умеет применять методики поиска, сбора и обработки информации: осуществлять критический анализ	Умеет применять методики поиска, сбора и обработки информации: осуществлять критический анализ и синтез информации, полученной из разных источников
Третий этап	ИД-3$_{УК-1}$ Владеть: методами поиска, сбора и обработки, критического анализа и синтеза информации: методикой системного подхода для решения поставленных задач	Не владеет	Владеет методами поиска, сбора и обработки, критического анализа	Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации	Владеет методами поиска, сбора и обработки, критического анализа и синтеза информации: методикой системного подхода для решения поставленных задач
Первый этап	ИД-1$_{ПК-9}$ Знать Методы обеспечения информационной безопасности на уровне БД	Не знает	Знает методы обеспечения информационной безопасности	Знать методику обеспечения информационной безопасности	Знает методы обеспечения информационной безопасности на уровне БД
Второй этап	ИД-2$_{ПК-9}$ Уметь анализировать угрозы информационной безопасности на уровне БД	Не умеет	Умеет анализировать угрозы	Умеет анализировать угрозы информационной безопасности	Уанализировать угрозы информационной безопасности на уровне БД

Этапы оценивания компетенции	Показатели достижения заданного уровня освоения компетенции	Критерии оценивания результатов обучения			
		2	**3**	**4**	**5**
Третий этап	ИД-3$_{ПК-9}$ Владеть способами обеспечения информационной безопасности на уровне БД	Не владеет	Владеет навыками работы с ПО	Владеет способами обеспечения информационной безопасности	Владеет способами обеспечения информационной безопасности на уровне БД

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 Пример лабораторной работы №1

Лабораторная работа №1. Основы безопасности в среде Windows

Обнаружение сетевых уязвимостей
Обнаружение сетевых уязвимостей
Обнаружение сетевых уязвимостей
Разработка плана мероприятий по защите информации предприятия
Разработка плана мероприятий по защите информации предприятия
Разработка плана мероприятий по защите информации предприятия
Разработка плана мероприятий по защите информации предприятия
Разработка плана мероприятий по защите информации предприятия
Разработка плана мероприятий по защите информации предприятия
Разработка плана мероприятий по защите информации предприятия
Работа с электронной цифровой подписью.
Работа с электронной цифровой подписью.
Работа с электронной цифровой подписью.

5.2 Пример лабораторной работы №2

Лабораторная работа №2. Встроенный межсетевой экран (firewall) Windows

5.3 Пример лабораторной работы №3

Лабораторная работа №3. Обнаружение сетевых уязвимостей

5.4. Пример лабораторной работы №4

Лабораторная работа №4. Разработка плана мероприятий по защите информации предприятия

5.5. Пример лабораторной работы №5

Лабораторная работа №5. Работа с электронной цифровой подписью.

5.6 Пример тем курсовых работ.

Темы курсовых работ по дисциплине «**Корпоративная безопасность**» курсовые работы не предусмотрены.

5.7 Вопросы к зачету по дисциплине «**Корпоративная безопасность**»

1. Понятия и определения защиты информации
2. Угрозы информационной безопасности
3. Технический канал утечки
4. Способы обеспечения безопасности информационной системы
5. Принципы комплексной защиты
6. Вирусные программы
7. Руткиты
8. Антивирусные и антиантивирусные технологии
9. Обнаружение и предотвращение вторжений
10. Стандарты информационной безопасности
11. Политика безопасности. (Понятие, структура, разработка)
12. Криптографическая защита информации (симметричные, ассиметричные системы)
13. Криптографическая защита информации (хеширование, цифровая подпись)
14. Разграничение доступа в информационной системе
15. Правовая защита информационных систем
16. Особенности обеспечения информационной безопасности в компьютерных сетях
17. Технология виртуальных частных сетей
18. Управление доступом аутентификация и идентификация

Тест

1. К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2. Виды информационной безопасности:

- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

3. Цели информационной безопасности – своевременное обнаружение, предупреждение:

- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

4. Основные объекты информационной безопасности:

- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

5. Основными рисками информационной безопасности являются:

- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

6. К основным принципам обеспечения информационной безопасности относится:

- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы

- Усиления защищенности всех звеньев системы

7. Основными субъектами информационной безопасности являются:

- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

8. К основным функциям системы безопасности можно отнести все перечисленное:

- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

9. ЭЦП – это:

- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор

10. Наиболее распространены угрозы информационной безопасности корпоративной системы:

- Покупка нелицензионного ПО
- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

11. Наиболее распространены угрозы информационной безопасности сети:

- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных

12. Утечкой информации в системе называется ситуация, характеризуемая:

- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

13. Угроза информационной системе (компьютерной сети) – это:

- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

14. Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке:

- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

15. Окончательно, ответственность за защищенность данных в компьютерной сети несет:

- Владелец сети
- Администратор сети
- Пользователь сети

16. Политика безопасности в системе (сети) – это комплекс:

- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

17. Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

18. Корпоративная безопасность – это:

- Комплекс мероприятий и процессов, направленных на обеспечение защиты информационных, экономических, научно-технических, правовых аспектов деятельности конкретной организации
- Политика безопасности предприятия, построенная на основе анализа наиболее вероятных угроз

19. Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

20. Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

21. К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания

22) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его