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

Инженерно-технический институт

Кафедра информационных технологий

УТВЕРЖДАЮ

Заведующий кафедрой ИТ

Ю.А. Столяренко

«28» августа 2023 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине

РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки
09.04.02 Информационные системы и технологии

Профиль подготовки
Защита информации в информационных системах

Квалификация (степень) выпускника: **магистр**

Форма обучения: **очная**

Год набора: **2023 г.**

Разработал:
Ст. преп. кафедры ИТ

/Д.С. Соколов
«28» августа 2023 г.

Тирасполь, 2023

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ» у обучающегося должны быть сформированы следующие компетенции:

Категория универсальных компетенций	**Код и наименование универсальной компетенции**	**Код и наименование индикатора достижения универсальной компетенции**
Универсальные компетенции выпускников и индикаторы их достижения		
Самоорганизация и саморазвитие (в том числе здоровье сбережение)	УК-6. Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	ИД-1$_{УК-6}$ Знать методики самооценки, самоконтроля и саморазвития с использованием подходов здоровье сбережения
		ИД-2$_{УК-6}$ Уметь решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности
		ИД-3$_{УК-6}$ Владеть технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровье сберегающих подходов и методик
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 Раздел 2	УК-6, ОПК-3	Контрольная работа №1 Лабораторные работы №1-2
РУБЕЖНАЯ АТТЕСТАЦИЯ	Раздел 3		Контрольная работа №2 Лабораторные работы №3-4
Промежуточная аттестация		Код контролируемой компетенции (или ее части)	Наименование оценочного средства
№1		УК-6, ОПК-3	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$_{УК-6}$ Знать методики самооценки, самоконтроля и саморазвития с использованием подходов здоровье сбережения	Не знает	Знает методики самооценки	Знает методики самооценки, самоконтроля и саморазвития	Знает методики самооценки, самоконтроля и саморазвития с использованием подходов здоровье сбережения
Второй этап	ИД-2$_{УК-6}$ Уметь решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; приме-	Не умеет	Умеет решать задачи собственного личностного и профессионального развития	Умеет решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности	Умеет решать задачи собственного личностного и профессионального развития, определять и реализовывать приоритеты совершенствования собственной деятельности; применять методики самооценки и самоконтроля; применять методики,

Этапы оценивания компетенции	Показатели достижения заданного уровня освоения компетенции	Критерии оценивания результатов обучения			
		2	**3**	**4**	**5**
	нять методики, позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности				позволяющие улучшить и сохранить здоровье в процессе жизнедеятельности
Третий этап	ИД-3$_{УК-6}$ Владеть технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровье сберегающих подходов и методик	Не владеет	Владеет технологиями и навыками управления своей познавательной деятельностью	Владеет технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля	Владеет технологиями и навыками управления своей познавательной деятельностью и ее совершенствования на основе самооценки, самоконтроля и принципов самообразования в течение всей жизни, в том числе с использованием здоровье сберегающих подходов и методик
Первый этап	ИД-1$_{ОПК-3}$ Знать принципы, методы и средства анализа и структурирования профессиональной информации	Не знает	Знать 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	Имеет навыки подготовки научных докладов, публикаций и аналитических обзоров	Имеет 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 Лабораторная работа №1. Тема: Анализ рисков информационной безопасности

5.2. Лабораторная работа №2. Тема: Построение концепции информационной безопасности предприятия

5.3. Лабораторная работа №3. Тема: Выполнение индивидуального задания

5.4. Лабораторная работа №4. Тема: Выполнение индивидуального задания

5.5 Перечень вопросов к зачету по предмету

1. Анализ возможных рисков безопасности предприятия и сценариев защиты
2. Выработка вариантов требований к системе информационной безопасности
3. Выбор основных решений по обеспечению режима информационной безопасности
4. Разработка нормативных документов по обеспечению бесперебойной работы компании
5. Разработка нормативной документации по системе управления информационной безопасностью
6. Принятие выработанных нормативных документов
7. Создание системы информационной безопасности
8. Системы обеспечения бесперебойной работы компании
9. Доработка принятых нормативных документов

Тестовые задания

1. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

1. служебная информация
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

2. Гарантия того, что конкретная информация доступна только тому кругу лиц, для которых она предназначена

1. конфиденциальность
2. целостность
3. доступность
4. аутентичность
5. аппелеруемость

3. Способность системы к целенаправленному приспособлению при изменении структуры, технологических схем или условий функционирования, которое спасает владельца АС от необходимости принятия кардинальных мер по полной замене средств защиты на новые.

1. принцип системности
2. принцип комплексности

3. принцип непрерывной защиты
4. принцип разумной достаточности
5. принцип гибкости системы

4. Комплекс превентивных мер по защите конфиденциальных данных и информационных процессов на предприятии это…

1. комплексное обеспечение ИБ
2. безопасность АС
3. угроза ИБ
4. атака на АС
5. политика безопасности

5. Автоматизированная система должна обеспечивать

1. надежность
2. доступность
3. целостность
4. контролируемость

6. Основными компонентами парольной системы являются

1. интерфейс администратора
2. хранимая копия пароля
3. база данных учетных записей
4. все варианты верны

7. Охрана персональных данных, государственной служебной и других видов информации ограниченного доступа это…

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

8. Система физической безопасности включает в себя следующие подсистемы:

1. оценка обстановки
2. скрытность
3. строительные препятствия
4. аварийная и пожарная сигнализация

9. К механическим системам защиты относятся:

1. проволока
2. стена
3. сигнализация
4. вы

10. Какие компоненты входят в комплекс защиты охраняемых объектов:

1. сигнализация
2. охрана
3. датчики
4. телевизионная система

11. К выполняемой функции защиты относится:

1. внешняя защита
2. внутренняя защита
3. все варианты верны

12. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Безопасность данных

13. Информация позволяющая ее обладателю при существующих или возможных обстоятельствах увеличивать доходы, сохранить положение на рынке товаров, работ или услуг это:

1. государственная тайна
2. коммерческая тайна
3. банковская тайна
4. конфиденциальная информация

14. Совокупность норм, правил и практических рекомендаций, регламентирующих работу средств защиты АС от заданного множества угроз безопасности:

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. атака на автоматизированную систему
5. политика безопасности

15. К достоинствам технических средств защиты относятся:

1. регулярный контроль
2. создание комплексных систем защиты
3. степень сложности устройства
4. Все варианты верны

16. К тщательно контролируемым зонам относятся:

1. рабочее место администратора
2. архив
3. рабочее место пользователя

17. К национальным интересам в информационной сфере относятся:

1. Реализация конституционных прав на доступ к информации
2. Защита информации, обеспечивающей личную безопасность
3. Защита независимости, суверенитета, государственной и территориальной целостности
4. Политическая экономическая и социальная стабильность
5. Сохранение и оздоровлении окружающей среды

18. Информационная безопасность это:

1. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз
2. Состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз
3. Состояние, когда не угрожает опасность информационным системам
4. Политика национальной безопасности страны

19. Что относится к классу информационных ресурсов:

1. Документы
2. Персонал
3. Организационные единицы
4. Промышленные образцы, рецептуры и технологии
5. Научный инструментарий

20. Гарантия того, что конкретная информация доступна только тому кругу лиц, для кого она предназначена:

1. конфиденциальность
2. доступность
3. аутентичность
4. целостность

21. Деятельность по предотвращению неконтролируемого распространения защищаемой информации от ее разглашения и несанкционированного доступа к защищаемой информации и от получения защищаемой информации:

1. защита информации от непреднамеренного воздействия
2. защита информации от несанкционированного воздействия
3. защита информации от несанкционированного доступа
4. *защита от утечки информации

22. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:

1. Информационная безопасность
2. Безопасность
3. Национальная безопасность
4. Защита информации

23. Охрана персональных данных, государственной, служебной и других видов информации ограниченного доступа это:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Защищенность потребителей информации
5. Безопасность данных

24. Реализация конституционных прав и свобод человека, обеспечение личной безопасности, повышение качества и уровня жизни это:

1. Интересы государства
2. Интересы государства в информационной сфере
3. Интересы личности
4. Интересы личности в информационной сфере
5. Интересы общества в информационной сфере

25. Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.

1. Комплексное обеспечение информационной безопасности
2. Безопасность АС
3. Угроза информационной безопасности
4. Атака на автоматизированную систему
5. Политика безопасности

26. Вся накопленная информация об окружающей нас дейст вительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производст венных, управленческих и других задач

1. Информационные ресурсы
2. Информационная система
3. Информационная сфера
4. Информационные услуги
5. Информационные продукты

27. Набор аппаратных и программных средств для обеспечения сохранности, доступности и конфиденциальности данных:

1. Защита информации
2. Компьютерная безопасность
3. Защищенность информации
4. Защищенность потребителей информации

28. Создание условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека в области получения

информации и пользования ею в целях обеспечения незыблемости конституционного строя , суверенитета и территориальной целостности это:

1. Интересы государства
2. Интересы государства в информационной сфере
3. Интересы личности
4. Интересы личности в информационной сфере
5. Интересы общества в информационной сфере

29. К какому уровню доступа информации относится следующая информация: «Авторское право, патентное право…»

1. Информация без ограничения права доступа
2. Информация с ограниченным доступом
3. Информация, распространение которой наносит вред интересам общества
4. Объект интеллектуальной собственности
5. Иная общедоступная информация

30. Состояние защищенности многонационального народа как носителя суверенитета и единственного источника власти:

1. Информационная безопасность
2. Безопасность
3. Защита информации
4. Национальная безопасность