

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сенченко Павел Васильевич
Должность: Проректор по учебной работе
Дата подписания: 25.10.2023 07:29:36
Уникальный программный ключ:
27e516f4c088deb62ba68945f4406e13fd454355

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

УПРАВЛЕНИЕ СРЕДСТВАМИ ЗАЩИТЫ ИНФОРМАЦИИ

Уровень образования: **высшее образование - бакалавриат**

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

Направленность (профиль) / специализация: **Безопасность автоматизированных систем**

Форма обучения: **очная**

Факультет: **Факультет безопасности (ФБ)**

Кафедра: **Кафедра комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС)**

Курс: **4**

Семестр: **7**

Учебный план набора 2021 года

Объем дисциплины и виды учебной деятельности

Виды учебной деятельности	7 семестр	Всего	Единицы
Лекционные занятия	18	18	часов
Лабораторные занятия	36	36	часов
в т.ч. в форме практической подготовки	12	12	часов
Курсовая работа	36	36	часов
в т.ч. в форме практической подготовки	12	12	часов
Самостоятельная работа	54	54	часов
Общая трудоемкость	144	144	часов
(включая промежуточную аттестацию)	4	4	з.е.

Формы промежуточной аттестация

	Семестр
Зачет	7
Курсовая работа	7

1. Общие положения

1.1. Цели дисциплины

1. Целью преподавания дисциплины является освоение методов мониторинга и управления программными средствами защиты информации, реализованными на основе клиент-серверной технологии.

1.2. Задачи дисциплины

1. Получение знаний и умений по методам сбора и аудита событий информационной безопасности в современных средствах защиты информации.

2. Получение умений и навыков централизованного управления клиентскими модулями средств защиты информации и реагирования на угрозы безопасности.

3. Получение знаний о методах контроля работоспособности и целостности клиентских модулей средств защиты информации.

4. Изучение методов контроля и оценки установленного программного и аппаратного обеспечения на защищаемых компьютерах в локальной сети.

5. Изучение методов обеспечения и контроля антивирусной защиты рабочих станций в сети организации.

2. Место дисциплины в структуре ОПОП

Блок дисциплин: Б1. Дисциплины (модули).

Часть блока дисциплин: Обязательная часть.

Модуль дисциплин: Модуль направленности (профиля) (major).

Индекс дисциплины: Б1.О.05.03.

Реализуется с применением электронного обучения, дистанционных образовательных технологий.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО и основной образовательной программой (таблица 3.1):

Таблица 3.1 – Компетенции и индикаторы их достижения

Компетенция	Индикаторы достижения компетенции
Универсальные компетенции	
-	-
Общепрофессиональные компетенции	
ОПК-2. Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	ОПК-2.1. Знает классификацию компьютерных систем, виды информационного взаимодействия и обслуживания, основы построения информационно-вычислительных систем
	ОПК-2.2. Умеет проводить анализ и выбор информационных технологий, программных средств системного и прикладного назначения для решения задач профессиональной деятельности
	ОПК-2.3. Владеет навыками использования информационно-коммуникационных технологий и программных средств системного и прикладного назначения для решения задач профессиональной деятельности

ОПК-4.1. Способен проводить организационные мероприятия по обеспечению безопасности информации в автоматизированных системах	ОПК-4.1.1. Знает содержание и порядок деятельности персонала по эксплуатации защищенных автоматизированных систем и систем защиты информации
	ОПК-4.1.2. Умеет определять подлежащие защите информационные ресурсы, определять параметры настройки программного обеспечения, осуществлять планирование и организацию работы персонала автоматизированной системы с учетом требований по защите информации
	ОПК-4.1.3. Владеет навыками разработки политики безопасности информации автоматизированных систем
ОПК-9. Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1. Знает основные понятия криптографии и криптографические методы защиты информации
	ОПК-9.2. Умеет определять наличие типовых технических каналов утечки информации, а также применять методики расчета и инструментального контроля показателей технической защиты информации на объектах информатизации
	ОПК-9.3. Владеет практическими навыками обоснованного выбора и использования СКЗИ при решении задач профессиональной деятельности
ОПК-12. Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.1. Знает номенклатуру и содержание нормативных правовых актов и нормативных методических документов, применяемых при проектировании защищенных автоматизированных систем
	ОПК-12.2. Умеет проводить анализ доступных информационных источников с целью выявления известных уязвимостей, используемых в системе защиты информации программных и программно-аппаратных средств
	ОПК-12.3. Владеет навыками проектирования элементов защищенных автоматизированных систем и разработки необходимой технической документации в области проектирования защищенных автоматизированных систем с учетом действующих нормативных и методических документов
Профессиональные компетенции	
-	-

4. Названия разделов (тем) дисциплины

Названия разделов (тем) дисциплины
7 семестр
1 Централизованное управление средствами защиты информации от несанкционированного доступа в локальной сети
2 Централизованная инвентаризация ресурсов локальной сети. Удаленный контроль работоспособности средств защиты информации на рабочих станциях
3 Централизованная защита от вирусов в локальной сети
4 Централизованный учет и управление средствами персональной идентификации и аутентификации
5 Анализ нормативных требований по управлению средствами защиты информации