

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н. Рева И. Л.

“ ” _____ г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ
Безопасность сетей электронных вычислительных машин

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

Курс: 4, семестр : 7

Факультет автоматики и вычислительной техники,

		Семестр
№	Вид деятельности	7
1	Всего зачетных единиц (кредитов)	4
2	Всего часов	144
3	Всего занятий в контактной форме, час.	94
4	Лекции, час.	36
5	Практические занятия, час.	0
6	Лабораторные занятия, час.	36
7	из них в активной и интерактивной форме, час.	18
8	Аттестация, час.	2
9	Консультации, час.	20
10	Самостоятельная работа, час.	50
11	Виды самостоятельной работы (курсовой проект, курсовая работа, РГЗ, подготовка к контрольной работе)	
12	Вид аттестации	ДЗ

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

ФГОС введен в действие приказом №1509 от 01.12.2016 г. , дата утверждения: 20.12.2016 г.

Место дисциплины в структуре учебного плана: Блок 1, базовая

Рабочая программа разработана на основе компетентностной модели выпускника по направлению (специальности): 10.05.03 Информационная безопасность автоматизированных систем

Рабочая программа обсуждена на заседании кафедры

ЗИ, протокол заседания кафедры №6 от 20.06.2017

Утверждена на совете факультета автоматики и вычислительной техники, протокол № 6 от 21.06.2017

Программу разработал:

доцент, к.т.н. Зырянов С. А.

Заведующий кафедрой:

с.н.с., к.т.н. Трушин В. А.

Ответственный за образовательную программу:

заведующий кафедрой Трушин В. А.

1. Внешние требования

Таблица 1.1

Компетенция ФГОС: ПК.11 способность разрабатывать политику информационной безопасности автоматизированной системы; в части следующих результатов обучения:	
з1. знать принципы формирования политики информационной безопасности в автоматизированных системах	
у1. уметь реализовывать политику безопасности автоматизированной системы	
Компетенция ФГОС: ПК.12 способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы; в части следующих результатов обучения:	
з2. знать методы управления информационной автоматизированной системой	
у2. уметь управлять информационной безопасностью автоматизированной системы	
у3. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	
Компетенция ФГОС: ПК.13 способность участвовать в проектировании средств защиты информации автоматизированной системы; в части следующих результатов обучения:	
у1. уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	
Компетенция ФГОС: ПК.17 способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации; в части следующих результатов обучения:	
з1. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
з2. знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	
у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем	
Компетенция ФГОС: ПК.19 способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы; в части следующих результатов обучения:	
у1. уметь администрировать подсистемы безопасности автоматизированных систем	
Компетенция ФГОС: ПК.2 способность создавать и исследовать модели автоматизированных систем; в части следующих результатов обучения:	
у1. уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач	
у2. уметь сформировать требования к автоматизированной системе	
Компетенция ФГОС: ПК.22 способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации; в части следующих результатов обучения:	
у1. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	
Компетенция ФГОС: ПК.23 способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа; в части следующих результатов обучения:	
у2. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
Компетенция ФГОС: ПК.9 способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности; в части следующих результатов обучения:	
з2. знать основные этапы разработки защищенных автоматизированных систем	

2. Требования НГТУ к результатам освоения дисциплины

Таблица 2.1

Результаты изучения дисциплины по уровням освоения (иметь представление, знать, уметь, владеть)	Формы организации занятий
--	----------------------------------

Безопасность сетей электронных вычислительных машин

ПК.2.y1 уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач	
1.использовать методы и средства защиты информации	Лекции; Лабораторные работы; Самостоятельная работа
ПК.2.y2 уметь сформировать требования к автоматизированной системе	
2.Организовывать построение системы защиты	Лекции
ПК.9.32 знать основные этапы разработки защищенных автоматизированных систем	
3.Этапы построения системы информационной безопасности компьютерных сетей	Лекции; Самостоятельная работа
ПК.11.31 знать принципы формирования политики информационной безопасности в автоматизированных системах	
4.Программно-аппаратные средства обеспечения информационной безопасности в компьютерных сетях	Лекции; Лабораторные работы; Самостоятельная работа
ПК.11.y1 уметь реализовывать политику безопасности автоматизированной системы	
5.Выполнять разработку компьютерных сетей с учетом требований по обеспечению безопасности	Лекции; Самостоятельная работа
ПК.12.32 знать методы управления информационной автоматизированной системой	
6.Криптографические методы, алгоритмы, протоколы	Лекции; Лабораторные работы; Самостоятельная работа
ПК.12.y2 уметь управлять информационной безопасностью автоматизированной системы	
7.использовать программно-аппаратных средств	Лекции; Лабораторные работы; Самостоятельная работа
ПК.12.y3 уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	
8.реализовывать политику безопасности компьютерной сети	Лекции; Лабораторные работы; Самостоятельная работа
ПК.13.y1 уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	
9.Использовать средства операционных систем	Лекции; Лабораторные работы; Самостоятельная работа
ПК.17.31 знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	
10.возможности технических средств перехвата информации	Лекции; Лабораторные работы; Самостоятельная работа
ПК.17.32 знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	
11.критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Лекции; Лабораторные работы; Самостоятельная работа
ПК.17.y2 уметь проводить инструментальный мониторинг защищенности автоматизированных систем	
12.использовать технические средства в профессиональной деятельности	Лекции; Лабораторные работы; Самостоятельная работа
ПК.19.y1 уметь администрировать подсистемы безопасности автоматизированных систем	
13.обеспечение эффективного и безопасного функционирования автоматизированных систем	Лекции; Лабораторные работы; Самостоятельная работа
ПК.22.y1 уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	

14.использовать средства операционных систем для обеспечения эффективного и безопасного функционирования автоматизированных систем	Лекции; Лабораторные работы; Самостоятельная работа
ПК.23.y2 уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	
15.использовать средства и способы обеспечения информационной безопасности	Лекции; Лабораторные работы; Самостоятельная работа

3. Содержание и структура учебной дисциплины

Таблица 3.1

Темы лекций	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Угрозы безопасности в АС				
1. Проблемы информационной безопасности компьютерных сетях	0	2	1, 3	Классификация угроз безопасности в информационных системах
Дидактическая единица: Модели безопасности компьютерных систем				
2. Модели безопасности компьютерных систем	0	2	2, 4	Идентификация, аутентификация и управление доступом
Дидактическая единица: Обеспечения безопасности сетевых ОС				
3. Безопасность сетевых ОС	0	4	5, 6	Сетевая аутентификация пользователя, макет системы защиты
4. Протокол сервиса Каталога LDAP , Active Directory	1	2	6, 7	стратегия именования объектов и планирование инфраструктуры
5. Инфраструктуры открытых ключей	1	2	10, 8, 9	Основные понятия архитектуры PKI
Дидактическая единица: Протоколы безопасного сетевого взаимодействия				
6. Протоколы сетевой аутентификации	1	2	11, 12	Протокол Kerberos
Дидактическая единица: Протоколы защищенных каналов				
7. Протоколы защищенных каналов	1	4	11, 13, 14	Тунелирование по уровням модели ВОС
Дидактическая единица: Технологии межсетевых экранов				
8. Технологии межсетевых экранов	1	2	10, 11, 14, 15	Особенности функционирования на различных уровнях модели OSI
Дидактическая единица: Технологии виртуальных защищенных сетей				
9. Технологии виртуальных защищенных сетей VPN	1	2	4, 6, 7	Основные виды технической реализации VPN.
Дидактическая единица: Защита удаленного доступа				
10. Централизованный контроль удаленного доступа	1	2	2, 3, 4, 5	Протоколы TACACS и RADIUS.
Дидактическая единица: Технологии обнаружения и предотвращения вторжений				
11. Технологии обнаружения и предотвращения вторжений	1	4	10, 11, 6, 7, 8	Функции безопасности системы обнаружения вторжений
Дидактическая единица: Безопасность промышленных систем и АС				

12. Безопасность промышленных систем и АС	1	4	10, 7, 8	Кибербезопасность АС
13. Многоуровневый подход к обеспечению информационной безопасности КИС	0	4	11, 12, 13	Подсистемы ИБ традиционных КИС и проблемы безопасности "облачной" инфраструктуры

Таблица 3.2

Темы лабораторных работ	Активные формы, час.	Часы	Ссылки на результаты обучения	Учебная деятельность
Семестр: 7				
Дидактическая единица: Обеспечения безопасности сетевых ОС				
1. Средства настройки безопасности MS Windows	1	4	1, 4	. Сетевая архитектура безопасности операционных систем
3. Домены Windows	1	4	11, 12, 9	Служба каталогов Active Directory
4. Сертификаты открытого ключа	1	4	11, 13	Концепция инфраструктуры безопасности
Дидактическая единица: Протоколы безопасного сетевого взаимодействия				
2. Защита на сетевом уровне - протокол IPSec	1	4	6, 7	Протоколы защищенных каналов
Дидактическая единица: Протоколы защищенных каналов				
5. Протоколы туннелирования канального уровня	1	4	12, 14, 15	протоколы PPTP и L2TP
6. Защита на сеансовом уровне	1	4	11, 12, 14	протоколы SSL, TLS и SOCKS
Дидактическая единица: Защита удаленного доступа				
9. Применение RADIUS аутентификации и управления доступом	1	4	11, 7, 8, 9	многоуровневая защита корпоративной информации
Дидактическая единица: Технологии обнаружения и предотвращения вторжений				
7. Функциональные возможности COB уровня узла	1	4	10, 8, 9	настройка функциональных требования безопасности COB уровня узла
8. Функциональные возможности COB уровня сети	1	4	10, 8, 9	настройка функциональных требования безопасности COB уровня сети

4. Самостоятельная работа обучающегося

№	Виды самостоятельной работы	Ссылки на результаты обучения	Часы на выполнение	Часы на консультации
Семестр: 7				
1	Подготовка к занятиям	10, 11, 3, 6	18	9
Работа с литературой, подробная информация приведена в приложении №1 : Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798 . - Загл. с экрана.				
2	Дополнительная учебная деятельность	10, 11, 12, 13, 14, 15, 7, 8, 9	16	7

, подробная информация приведена в приложении №1 : Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.

3	Подготовка к аттестации	1, 10, 11, 12, 14, 3, 4, 5, 6, 7	16	4
---	-------------------------	-------------------------------------	----	---

, подробная информация приведена в приложении №2 : Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.

5. Технология обучения

Для организации и контроля самостоятельной работы обучающихся, а также проведения консультаций применяются информационно-коммуникационные технологии (табл. 5.1).

Таблица 5.1

Деятельность	Информационно-коммуникационные технологии
Информирование	Портал НГТУ; Среда электронного обучения НГТУ
Консультирование	Среда электронного обучения НГТУ
Контроль	Среда электронного обучения НГТУ
Размещение учебных материалов	Среда электронного обучения НГТУ

6. Правила аттестации обучающихся по учебной дисциплине

Для аттестации обучающихся по дисциплине используется балльно-рейтинговая система (БРС), позволяющая выставять оценки по традиционной шкале и 15-уровневой ECTS. Краткая информация о БРС приведена в табл. 6.1.

Таблица 6.1

Оцениваемые виды деятельности обучающихся	Мин. балл	Максимальный балл
Семестр: 7		
<i>Лабораторная:</i>	5	80
Контролирующие материалы - список вопросов		
<i>Зачет:</i>	10	20
Контролирующие материалы - список вопросов		

В таблице 6.2 представлено соответствие форм контроля заявляемым требованиям к результатам освоения дисциплины.

Таблица 6.2

Коды компетенций ФГОС	Результаты обучения	Формы контроля	
		Защита ЛР	Зачет
ПК.11	31. знать принципы формирования политики информационной безопасности в автоматизированных системах	+	+
	y1. уметь реализовывать политику безопасности автоматизированной системы		+
ПК.12	32. знать методы управления информационной автоматизированной системой	+	+

	у2. уметь управлять информационной безопасностью автоматизированной системы	+	+
	у3. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы		+
ПК.13	у1. уметь проводить выбор программно-аппаратных средств обеспечения информационной безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	+	+
ПК.17	з1. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	+	+
	з2. знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности		+
	у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем	+	+
ПК.19	у1. уметь администрировать подсистемы безопасности автоматизированных систем		+
ПК.2	у1. уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач	+	+
	у2. уметь сформировать требования к автоматизированной системе		+
ПК.22	у1. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе		+
ПК.23	у2. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	+	+
ПК.9	з2. знать основные этапы разработки защищенных автоматизированных систем		+

Фонд оценочных средств по дисциплине представлен в приложении № 1 к рабочей программе.

7. Литература

Основная литература

1. Платонов В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей : [учебное пособие для вузов] / В. В. Платонов. - М., 2006. - 238, [1] с. : ил., табл.
2. UNIX: руководство системного администратора : [пер. с англ.] / Эви Немет, Гарт Снайдер, Скотт Сибасс, Трент Р. Хейн. - М. [и др.], 2008. - 923, [1] с. : ил.
3. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : [учебное пособие для вузов по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем"] / В. Олифер, Н. Олифер. - СПб. [и др.], 2010. - 943 с. : ил.
4. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы : [учебное пособие для вузов по направлению "Информатика и вычислительная техника" и по специальностям "Вычислительные машины, комплексы, системы и сети", "Программное обеспечение вычислительной техники и автоматизированных систем"] / В. Олифер, Н. Олифер. - СПб. [и др.], 2012. - 943 с. : ил.

5. Воробьев Л. В. Системы и сети передачи информации : [учебное пособие для вузов по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем"] / Л. В. Воробьев, А. В. Давыдов, Л. П. Щербина. - М., 2009. - 328, [1] с. : схемы
6. Microsoft Windows Server 2008 R2 : полное руководство : [уровень пользователей: средней и высокой квалификации] / Рэнд Моримото [и др.] ; техн. ред. Гая Ярдени ; [пер. с англ. Я. П. Волковой и др.]. - М. [и др.], 2012. - 1455 с. : ил.
7. Шелухин О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии) : [учебное пособие для вузов по направлению подготовки 210700 - "Информационные технологии и системы связи" квалификации (степени) "бакалавр" и "магистр"] / О. И. Шелухин, Д. Ж. Сакалема, А. С. Филинова ; под ред. О. И. Шелухина. - Москва, 2013. - 220 с. : ил.

Интернет-ресурсы

1. ЭБС НГТУ : <http://elibrary.nstu.ru/>
2. ЭБС «Издательство Лань» : <https://e.lanbook.com/>
3. ЭБС IPRbooks : <http://www.iprbookshop.ru/>
4. ЭБС "Znaniy.com" : <http://znaniy.com/>
5. :

8. Методическое и программное обеспечение

8.1 Методическое обеспечение

1. Зырянов С. А. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : электронный учебно-методический комплекс / С. А. Зырянов ; Новосиб. гос. техн. ун-т. - Новосибирск, [2014]. - Режим доступа: http://elibrary.nstu.ru/source?bib_id=vtls000208798. - Загл. с экрана.

8.2 Специализированное программное обеспечение

- 1 Windows
- 2 Office

9. Материально-техническое обеспечение

Презентационное оборудование

№	Наименование	Назначение
1	Презентационное оборудование (мультимедиа-проектор, экран, компьютер для управления)	Презентация лекционных материалов

Компьютерный класс

№	Наименование	Назначение
1	Компьютерный класс (Компьютеры объединены в локальную сеть с выходом в Internet)	Выполнение ЛР

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра защиты информации

“УТВЕРЖДАЮ”
ДЕКАН АВТФ
к.т.н., доцент И.Л. Рева
“ ” _____ Г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

УЧЕБНОЙ ДИСЦИПЛИНЫ

Безопасность сетей электронных вычислительных машин

Образовательная программа: 10.05.03 Информационная безопасность автоматизированных систем, специализация: Информационная безопасность автоматизированных систем критически важных объектов

1. Обобщенная структура фонда оценочных средств учебной дисциплины

Обобщенная структура фонда оценочных средств по дисциплине **Безопасность сетей электронных вычислительных машин** приведена в Таблице.

Таблица

Формируемые компетенции	Показатели сформированности компетенций (знания, умения, навыки)	Темы	Этапы оценки компетенций	
			Мероприятия текущего контроля (курсовой проект, РГЗ(Р) и др.)	Промежуточная аттестация (экзамен, зачет)
ПК.11/ПК способность разрабатывать политику информационной безопасности автоматизированной системы	з1. знать принципы формирования политики информационной безопасности в автоматизированных системах	Модели безопасности компьютерных систем Средства настройки безопасности MS Windows Технологии виртуальных защищенных сетей VPN Централизованный контроль удаленного доступа	Отчет по лабораторной работе, разделы...	Зачет, вопросы...
ПК.11/ПК	у1. уметь реализовывать политику безопасности автоматизированной системы	Безопасность сетевых ОС Централизованный контроль удаленного доступа		Зачет, вопросы...
ПК.12/ПК способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	з2. знать методы управления информационной автоматизированной системой	Безопасность сетевых ОС Защита на сетевом уровне - протокол IPSec Протокол сервиса Каталога LDAP , Active Directory Технологии виртуальных защищенных сетей VPN Технологии обнаружения и предотвращения вторжений	Отчет по лабораторной работе, разделы...	Зачет, вопросы...
ПК.12/ПК	у2. уметь управлять информационной безопасностью автоматизированной системы	Безопасность промышленных систем и АС Защита на сетевом уровне - протокол IPSec Применение RADIUS аутентификации и управления доступом Протокол сервиса Каталога LDAP , Active Directory Технологии виртуальных защищенных сетей VPN Технологии обнаружения и предотвращения вторжений	Отчет по лабораторной работе, разделы...	Зачет, вопросы...
ПК.12/ПК	у3. уметь разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	Безопасность промышленных систем и АС Инфраструктуры открытых ключей Технологии обнаружения и предотвращения вторжений		Зачет, вопросы...
ПК.13/ПК способность участвовать в проектировании средств защиты	у1. уметь проводить выбор программно-аппаратных средств обеспечения информационной	Домены Windows Инфраструктуры открытых ключей Применение RADIUS аутентификации и управления доступом Функциональные	Отчет по лабораторной работе, разделы...	Зачет, вопросы...

информации автоматизированной системы	безопасности для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы	возможности СОВ уровня сети Функциональные возможности СОВ уровня узла		
ПК.17/КА способность проводить инструментальный мониторинг защищенности информации в автоматизированной системе и выявлять каналы утечки информации	31. знать методы мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем	Безопасность промышленных систем и АС Инфраструктуры открытых ключей Технологии межсетевых экранов Технологии обнаружения и предотвращения вторжений Функциональные возможности СОВ уровня сети Функциональные возможности СОВ уровня узла	Отчет по лабораторной работе, разделы...	Зачет, вопросы...
ПК.17/КА	32. знать автоматизированную систему как объект информационного воздействия, критерии оценки ее защищенности и методы обеспечения ее информационной безопасности	Многоуровневый подход к обеспечению информационной безопасности КИС Протоколы защищенных каналов Протоколы сетевой аутентификации Технологии межсетевых экранов Технологии обнаружения и предотвращения вторжений		Зачет, вопросы...
ПК.17/КА	у2. уметь проводить инструментальный мониторинг защищенности автоматизированных систем	Домены Windows Защита на сеансовом уровне Многоуровневый подход к обеспечению информационной безопасности КИС Протоколы сетевой аутентификации Протоколы туннелирования канального уровня	Отчет по лабораторной работе, разделы...	Зачет, вопросы...
ПК.19/ОУ способность разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированной системы	у1. уметь администрировать подсистемы безопасности автоматизированных систем	Многоуровневый подход к обеспечению информационной безопасности КИС Протоколы защищенных каналов		Зачет, вопросы...
ПК.2/НИ способность создавать и исследовать модели автоматизированных систем	у1. уметь подобрать составляющие элементы автоматизированной системы для реализации поставленных задач	Проблемы информационной безопасности компьютерных сетей Средства настройки безопасности MS Windows	Отчет по лабораторной работе, разделы...	Зачет, вопросы...
ПК.2/НИ	у2. уметь сформировать требования к автоматизированной системе	Модели безопасности компьютерных систем Централизованный контроль удаленного доступа		Зачет, вопросы...

ПК.22/ОУ способность участвовать в формировании политики информационной безопасности организации и контролировать эффективность ее реализации	у1. уметь формировать и настраивать политику безопасности распространенных операционных систем, а также локальных вычислительных сетей, построенных на их основе	Протоколы защищенных каналов Технологии межсетевых экранов		Зачет, вопросы...
ПК.23/ОУ способность формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	у2. уметь осуществлять меры противодействия нарушениям сетевой безопасности с использованием различных программных и аппаратных средств защиты	Протоколы туннелирования канального уровня Технологии межсетевых экранов	Отчет по лабораторной работе, разделы...	Зачет, вопросы...
ПК.9/ПК способность участвовать в разработке защищенных автоматизированн ых систем в сфере профессиональной деятельности	з2. знать основные этапы разработки защищенных автоматизированн ых систем	Проблемы информационной безопасности компьютерных сетей Централизованный контроль удаленного доступа		Зачет, вопросы...

2. Методика оценки этапов формирования компетенций в рамках дисциплины.

Промежуточная аттестация по дисциплине проводится в 7 семестре - в форме дифференцированного зачета, который направлен на оценку сформированности компетенций ПК.11/ПК, ПК.12/ПК, ПК.13/ПК, ПК.17/КА, ПК.19/ОУ, ПК.2/НИ, ПК.22/ОУ, ПК.23/ОУ, ПК.9/ПК.

Зачет проводится в устной (письменной) форме, по билетам (тестам).

Кроме того, сформированность компетенций проверяется при проведении мероприятий текущего контроля, указанных в таблице раздела 1.

Общие правила выставления оценки по дисциплине определяются балльно-рейтинговой системой, приведенной в рабочей программе учебной дисциплины.

На основании приведенных далее критериев можно сделать общий вывод о сформированности компетенций ПК.11/ПК, ПК.12/ПК, ПК.13/ПК, ПК.17/КА, ПК.19/ОУ, ПК.2/НИ, ПК.22/ОУ, ПК.23/ОУ, ПК.9/ПК, за которые отвечает дисциплина, на разных уровнях.

Общая характеристика уровней освоения компетенций.

Ниже порогового. Уровень выполнения работ не отвечает большинству основных требований, теоретическое содержание курса освоено частично, пробелы могут носить существенный характер, необходимые практические навыки работы с освоенным материалом сформированы не достаточно,

большинство предусмотренных программой обучения учебных заданий не выполнены или выполнены с существенными ошибками.

Пороговый. Уровень выполнения работ отвечает большинству основных требований, 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 виды заданий выполнены с ошибками.

Базовый. Уровень выполнения работ отвечает всем основным требованиям, 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 из выполненных заданий, возможно, содержат ошибки.

Продвинутый. Уровень выполнения работ отвечает всем требованиям, 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.

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»
Кафедра защиты информации

Паспорт зачета

по дисциплине «Безопасность сетей электронных вычислительных машин», 7 семестр

1. Методика оценки

Зачет проводится в устной (письменной) форме, по билетам. Билет формируется по следующему правилу: первый вопрос выбирается из диапазона вопросов 1-33, второй вопрос из диапазона вопросов 34-66 (список вопросов приведен ниже). В ходе экзамена преподаватель вправе задавать студенту дополнительные вопросы из общего перечня (п. 4).

Форма билета для зачета

НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет АВТФ

Билет № _____

к зачету по дисциплине «Безопасность сетей электронных вычислительных машин»

1. Вопрос 1
2. Вопрос 2.

Утверждаю: зав. кафедрой _____ должность, ФИО
(подпись)
(дата)

Критерии оценки

- Ответ на билет для зачета считается **неудовлетворительным**, если студент при ответе на вопросы не дает определений основных понятий, не способен показать причинно-следственные связи явлений, при решении задачи допускает принципиальные ошибки, оценка составляет *50 баллов*.
- Ответ на билет для зачета засчитывается на **пороговом** уровне, если студент при ответе на вопросы дает определение основных понятий, может показать причинно-следственные связи явлений, при решении задачи допускает непринципиальные ошибки, например, вычислительные, оценка составляет *60 баллов*.
- Ответ на билет для зачета билет засчитывается на **базовом** уровне, если студент при ответе на вопросы формулирует основные понятия, законы, дает характеристику процессов, явлений, проводит анализ причин, условий, может представить

качественные характеристики процессов, не допускает ошибок при решении задачи, оценка составляет 75 баллов.

- Ответ на билет для зачета билет засчитывается на **продвинутом** уровне, если студент при ответе на вопросы проводит сравнительный анализ подходов, проводит комплексный анализ, выявляет проблемы, предлагает механизмы решения, способен представить количественные характеристики определенных процессов, приводит конкретные примеры из практики, не допускает ошибок и способен обосновать выбор метода решения задачи, оценка составляет 95 баллов.

2. Шкала оценки

Зачет считается сданным, если сумма баллов по всем заданиям билета оставляет не менее 50 баллов (из 100 возможных).

В общей оценке по дисциплине баллы за зачет учитываются в соответствии с правилами балльно-рейтинговой системы, приведенными в рабочей программе дисциплины.

3. Вопросы к зачету по дисциплине «Безопасность сетей электронных вычислительных машин»

1. Анализ угроз информационной безопасности. Классификация угроз безопасности в информационных системах.
2. Угрозы несанкционированного доступа к информации в информационной системе.
3. Характеристика источников угроз несанкционированного доступа в информационной системе и результатов несанкционированного или случайного доступа.
4. Характеристика уязвимостей информационной системы. Уязвимости отдельных протоколов стека протоколов TCP/IP.
5. Характеристика угроз безопасности, реализуемых с использованием протоколов межсетевого взаимодействия. Классификационная схема угроз. Первичные признаки классификации. Назвать наиболее часто реализуемых в настоящее время угрозы.
6. Угроза «Анализ сетевого трафика». Сканирование сети. Угроза выявления пароля. Отказ в обслуживании.
7. Подмена доверенного объекта сети и передача по каналам связи сообщений от его имени с присвоением его прав доступа.
8. Навязывание ложного маршрута сети.
9. Внедрение ложного объекта сети.
10. Удаленный запуск приложений
11. Модели безопасности компьютерных систем. Модели дискреционного разграничения доступа.
12. Модели безопасности компьютерных систем. Модели мандатного разграничения доступа.
13. Модели безопасности компьютерных систем. Модели ролевого разграничения доступа.
14. Модели безопасности компьютерных систем. Модели безопасности информационных потоков.
15. Модели безопасности компьютерных систем. Субъектно ориентированная модель изолированной программной среды.
16. Идентификация, аутентификация и управление доступом. Аутентификация, авторизация и администрирование действий пользователей.
17. Биометрическая идентификация и аутентификация. Обобщенная биометрическая система. Функции обобщенной биометрической системы.

18. Биометрические профили для взаимодействия и обмена данными. Общая архитектура биометрической системы и биометрические профили информационной безопасностью. ГОСТ ISO/IEC 24713-1-2013.
19. Вопросы обеспечения безопасности в операционной среде Windows. Аутентификация пользователей при удаленном доступе.
20. Механизм идентификации и аутентификации в ОС Windows. Процесс Winlogon.
21. Механизм идентификации и аутентификации в ОС Windows. Локальная аутентификация пользователя в Windows.
22. Механизм идентификации и аутентификации в ОС Windows. Сетевая аутентификация пользователя в Windows.
23. Механизм идентификации и аутентификации в ОС Windows. Макет системы защиты от несанкционированного доступа.
24. Протокол сервиса Каталога LDAP (Lightweight Directory Access Protocol).
25. Служба каталогов Active Directory. Архитектура AD, стратегия именования объектов и планирование инфраструктуры.
26. Инфраструктуры открытых ключей. Доверие в сфере электронных коммуникаций.
27. Инфраструктуры открытых ключей. Концепция инфраструктуры безопасности
28. Инфраструктуры открытых ключей. Цель и сервисы инфраструктуры безопасности.
29. Инфраструктуры открытых ключей. Механизмы аутентификации
30. Инфраструктуры открытых ключей. Основные компоненты PKI.
31. Инфраструктуры открытых ключей. Основные сервисы PKI.
32. Инфраструктуры открытых ключей. Сервисы безопасности PKI
33. Инфраструктуры открытых ключей. Модели и механизмы доверия
34. Инфраструктуры открытых ключей. Сертификаты открытых ключей.
35. Классификация сертификатов и управление ими.
36. Инфраструктуры открытых ключей. Основные понятия архитектуры PKI.
37. Инфраструктуры открытых ключей. Механизмы распространения информации PKI
38. Инфраструктуры открытых ключей. Политики, регламент и процедуры PKI. Политика безопасности и способы ее реализации.
39. Инфраструктуры открытых ключей. Сервисы, базирующиеся на PKI. Механизмы необходимые для сервисов. Условия функционирования сервисов.
40. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Защищенная электронная почта S/MIME.
41. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Средства безопасности транспортного уровня.
42. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Средства безопасности IP-уровня .
43. Инфраструктуры открытых ключей. Приложения, базирующиеся на PKI. Типовые сценарии использования PKI.
44. Протоколы безопасного сетевого взаимодействия. Протоколы сетевой аутентификации.
45. Протоколы безопасного сетевого взаимодействия. Протокол Kerberos.
46. Протоколы защищенных каналов. Защита на канальном уровне - протоколы PPTP и L2TP.
47. Протоколы защищенных каналов. Защита на сетевом уровне - протокол IPSec.
48. Протоколы защищенных каналов. Защита на сеансовом уровне - протоколы SSL, TLS и SOCKS.
49. Протоколы защищенных каналов.. Протокол SSH.
50. Протоколы защищенных каналов. Защита беспроводных сетей.
51. Технологии межсетевых экранов. Функции межсетевых экранов
52. Технологии межсетевых экранов. Особенности функционирования межсетевых экранов на различных уровнях модели OSI

53. Технологии межсетевых экранов. Схемы сетевой защиты на базе межсетевых экранов
54. Технологии виртуальных защищенных сетей VPN. Концепция построения виртуальных защищенных сетей VPN. Классификация VPN .
55. Технологии виртуальных защищенных сетей VPN. VPN-решения для построения защищенных сетей.
56. Технологии виртуальных защищенных сетей VPN. Основные виды технической реализации VPN.
57. Защита удаленного доступа. Централизованный контроль удаленного доступа. Протоколы TACACS и RADIUS.
58. Технологии обнаружения и предотвращения вторжений.
59. Принципы многоуровневой защиты корпоративной информации.
60. Корпоративная информационная система с традиционной структурой
61. Многоуровневый подход к обеспечению информационной безопасности КИС
62. Подсистемы информационной безопасности традиционных КИС
63. Безопасность «облачных» вычислений
64. Основные проблемы безопасности «облачной» инфраструктуры
65. Средство защиты в виртуальных средах.
66. Безопасность промышленных систем и АСУ ТП.