Приложение 3

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«17» апреля 2024 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.О.34 Основы информационной безопасности**

Направление подготовки **09.03.02 Информационные системы и технологии**

Направленность (профиль) подготовки **Электронный инжиниринг**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №38 от «18» апреля 2023 г.

Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 7 от «27» февраля 2023 г.

И.О. зав. кафедрой _____ Колесник С.Н.

Иркутск 2023 г.

Содержание

I. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Целью изучения учебной дисциплины «Информационная безопасность» является формирование у студентов знаний о принципах обеспечения информационной безопасности в информационных сетях.

Задачами освоения учебной дисциплины являются получение:

– знаний об основных видах угроз информационной безопасности,

– знаний о наиболее важных сервисах и механизмах защиты информации,

– навыков работы с программно-аппаратными средствами защиты информации.

II. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Информационная безопасность» входит в вариативную часть дисциплин по выбору профессионального цикла ОПОП по направлению 03.03.03 "Радиофизика".

Изучение курса предполагает наличие полученных на предыдущем уровне образования основных знаний по дисциплинам: "Теория информации и базы данных", "Основы цифровой электроники и схемотехники", "Компьютерные вычислительные сети".

Полученные в процессе изучения курса знания и навыки могут быть использованы в процессе выполнения производственной практики и выпускной квалификационной работы, и в дальнейшей профессиональной работе.

III. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **09.03.02 Информационные системы и технологии**.

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

Компетенция	Индикаторы компетенций	Результаты обучения
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	*ИДК$_{ОПК-3.3}$* Выполняет требования информационной безопасности при решении профессиональных задач	**Знать:** основные виды и типы угроз информационной безопасности, наиболее важные сервисы и механизмы информационной безопасности, основные способы предотвращения удаленных атак на информационные системы **Уметь:** самостоятельно использовать современные компьютерные сети, программные продукты и ресурсы информационно-телекоммуникационной сети «Интернет» для получения и изучения материалов в области обеспечения информационной безопасности **Владеть**: навыками настройки программных и аппаратных средств обеспечения информационной безопасности

IV. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единиц, 108 часов,
Форма промежуточной аттестации: зачёт

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Лабораторное занятие	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Раздел № 1. Общие вопросы информационной безопасности	8	7		4			3	Устный текущий контроль
2	Раздел №2. Механизмы защиты информации	8	26,5		4	10	0,5	12	Устный текущий контроль
3	Раздел №3. Программно-аппаратные средства обеспечения информационной безопасности информационных сетей	8	66,5		4	50	0,5	12	Устный текущий контроль

4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
8	Раздел № 1. Общие вопросы информационной безопасности	повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов самостоятельная подготовка к выполнению практических работ.	Весь семестр	3	Устный опрос	Литература из библиотеки, Интернет
8	Раздел №2. Механизмы защиты информации		Весь семестр	12		
8	Раздел №3. Программно-аппаратные средства обеспечения информационной безопасности информационных сетей		Весь семестр	12		
Общий объем самостоятельной работы по дисциплине (час)				**27**		

4.3. Содержание учебного материала

Раздел № 1. Общие вопросы информационной безопасности

Основные понятия и определения в области информационной безопасности. Общая классификация угроз информационной безопасности. Виды угроз. Основные типы атак. Характер происхождения угроз (умышленные и естественные факторы). Источники угроз. Предпосылки появления угроз. Классы каналов несанкционированного получения информации. Причины нарушения целостности информации.

Раздел №2. Механизмы защиты информации

Формирование системы информационной безопасности. Механизмы защиты информации. Аутентификация и управление идентификациями. Антивирусные средства защиты информации. Криптографические методы защиты информации. Симметричное шифрование, ассиметричное шифрование, хэш-функции. Способы предотвращения удаленных атак на информационные системы. Управление доступом.

Раздел №3. Программно-аппаратные средства обеспечения информационной безопасности информационных сетей.

Сегментирование сетей на канальном уровне, VLAN. Технологии межсетевых экранов. Виртуальные частные сети VPN. Фильтрация трафика. Технология преобразования сетевых адресов NAT. Системы обнаружения и предотвращения проникновений IDPS. Ограничения IDPS. Технологии туннелирования. Акустические, электромагнитные средства защиты информации.

4.3.1 Перечень семинарских, практических занятий и лабораторных работ

№ п/н	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции (индикаторы)*
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1	2	Изучение программы «РЕВИЗОР -1 XP»	5		Устный текущий контроль	ОПК-3 ИДК$_{ОПК-3.3}$
2	2	Изучение программы «СТРАЖ NT»	5		Устный текущий контроль	ОПК-3 ИДК$_{ОПК-3.3}$
3	3	Изучение программы «Гроза-К», «Ревизор-2XP»	5		Устный текущий контроль	ОПК-3 ИДК$_{ОПК-3.3}$
4	3	Изучение программы «SecretNET»	5		Устный текущий контроль	ОПК-3 ИДК$_{ОПК-3.3}$
5	3	Изучение аппаратуры «NR-900EMS», «Аврора-3», «Крона-ПРО».	10		Устный текущий контроль	ОПК-3 ИДК$_{ОПК-3.3}$
6	3	Изучение аппаратуры	10		Устный текущий	ОПК-3 ИДК$_{ОПК-3.3}$

		«Соната-Р2»			контроль	
7	3	Изучение системы «Талис-нч – лайт»	10		Устный текущий контроль	ОПК-3 ИДК$_{ОПК-3.3}$
8	3	Изучение аппаратуры «Ладья-ИВТ», «Кедр-1М»	10		Устный текущий контроль	ОПК-3 ИДК$_{ОПК-3.3}$

4.3.2 Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1	2	3	4	5
1	Общие вопросы информационной безопасности	- повторение и углубленное изучение учебного материала лекции, ПЗ с использованием конспекта лекций, литературы, Интернет - ресурсов - самостоятельная подготовка к выполнению практических работ.	ОПК-3	ИДК$_{ОПК-3.3}$
2	Механизмы защиты информации			
3	Программно-аппаратные средства обеспечения информационной безопасности информационных сетей			

4.4. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа бакалавров – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя (научного руководителя (консультанта)), в ходе которой бакалавр активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи.

4.5. Примерная тематика курсовых работ

Выполнение курсовых работ не предусмотрено учебным планом

V. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) перечень литературы

1. Нестеров, С.А. Основы информационной безопасности. [Электронный ресурс] : учеб. пособие — Электрон. дан. — СПб. : Лань, 2017. — 324 с. (Режим доступа: ЭБС "Лань". - Неогранич. доступ). https://e.lanbook.com/book/90153

2. Андрончик А.Н. Мониторинг и управление в компьютерных сетях : учеб. пособие / А. Н. Андрончик. - Иркутск: Изд-во ИГУ, 2013. - 107 с. - ISBN 978-5-9624-0790-6 (30 экз.)

3. Агафонов А.В. Технологии межсетевого экранирования [Текст] : [учеб.

пособие] / А. В. Агафонов, А. Н. Андрончик, Ю. Д. Корольков ; Иркутский гос. ун-т, Ин-т математики, эконом. и информ. - Иркутск : Изд-во ИГУ, 2013. - 107 с. : ил. ; 25 см. - Библиогр.: с. 101. - ISBN 978-5-9624-0796-8 (30 экз.)

4. Шаньгин В. Ф. Защита компьютерной информации. Эффективные методы и средства [Текст] : учеб. пособие / В. Ф. Шаньгин. - М. : ДМК Пресс, 2010. - 542 с. ; 24 см. - Библиогр.: с. 524-529. - Предм. указ.: с. 530-542. - ISBN 978-5-94074-518-1(25 экз.)

б) периодические издания

в) список авторских методических разработок

г) базы данных, информационно-справочные и поисковые системы

1. Научная библиотека ИГУ *http://library.isu.ru/ru/resources/edu_resources/index.html*
2. БД книг и продолжающихся изданий http://ellibnb.library.isu.ru/cgi-bin/irbis64r_15/cgiirbis_64.htm?LNG=&C21COM=F&I21DBN=IRCAT&P21DBN=IRCAT
3. Электронный читальный зал «БиблиоТех» https://isu.bibliotech.ru/
4. Электронная библиотечная система «Издательство «Лань» http://e.lanbook.com
5. Электронная библиотечная система «РУКОНТ» http://rucont.ru

VI. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Экран и проектор для демонстрации видеоматериалов, доска.

6.2. Программное обеспечение:

1. ABBY PDF Transformer 3.0 Пакет из 10 неименных лицензий Per Seat (10лиц.) EDU. Код позиции: AT30-1S1P10-102 Котировка № 03-165-11 от 23.11.2011. Бессрочно.
2. Microsoft OfficeProPlus 2013 RUS OLP NL Acdmc. Контракт № 03-013-14 от 08.10.2014.Номер Лицензии Microsoft 45936786. Бессрочно.
3. WinPro10 Rus Upgrd OLP NL Acdmc. Сублицензионный договор № 502 от 03.03.2017 Счет № ФРЗ- 0003367 от 03.03.2017 Акт № 4496 от 03.03.2017 Лицензия № 68203568. Бессрочно.
4. Kaspersky Free (ежегодно обновляемое ПО). Условия использования по ссылке: http://www.kaspersky.ru/free-antivirus/ . Бессрочно.
5. Лицензионный пакет Lab VIEW фирмы National Instruments.
6. Лицензионное программное обеспечение базовой станции NI ELVIS-II.

Браузеры MS Internet Explorer, Mozilla Firefox, Opera, ПО OpenVPN, ПО GNU Privacy Guard, ПО, поставляемое с оборудованием D-Link. Специализированное программное обеспечение «РЕВИЗОР -1 XP», «СТРАЖ NT», «Гроза-К», «Ревизор-2XP», «SecretNET».

6.3. Технические и электронные средства:

Компьютерный класс с установленным ПО MS Internet Explorer, Mozilla Firefox, Opera, сетевое оборудование D-Link: беспроводные маршрутизаторы, сетевые экраны, точки доступа, управляемые коммутаторы, коммутаторы 3-го уровня, сетевое файлохранилище, IP-камеры для проведения практических и лабораторных занятий. Оборудование «NR-900EMS», «Аврора-3», «Крона-ПРО», «Соната-Р2», «Талис-нч –лайт», «Ладья-ИВТ», «Кедр-1М». Аудитория с мультимедийным проектором для проведения лекционных занятий. Офисное оборудование для оперативного размножения иллюстративного и раздаточного лекционного материала.

VII. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Теоретические занятия дисциплины представлены в виде лекций. Чтение лекций по данной дисциплине проводится как в классической форме, так и с использованием мультимедийных презентаций. Слайд-конспект курса лекций предназначен для более глубокого усвоения материала при изучении разделов, связанных с технической частью курса. Презентация позволяет преподавателю очень хорошо иллюстрировать лекцию не только схемами и рисунками, которые есть в учебных пособиях, но и полноцветными фотографиями, рисунками и т.д. Студентам предоставляется возможность копирования презентаций для самоподготовки. Чтение лекций по темам также предполагает разбор конкретных ситуаций в качестве примеров, подкрепляющих теоретический материал.

Практические навыки работы программно-аппаратными средствами обеспечения информационной безопасности информационных сетей усваиваются в ходе проведения практических занятий. Любая практическая работа должна включать глубокую самостоятельную внеаудиторную проработку теоретического материала. Для этого преподаватель выдает студентам задания для выполнения практических и лабораторных работ.

VIII. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Текущий контроль направлен на выявление сформированности компетенций ОПК-3 и реализуется в виде устного контрольного опроса на практических занятиях и КСР и устного отчета по работе с программно-аппаратными средствами обеспечения информационной безопасности информационных сетей на практических и лабораторных занятиях.

За посещение одного вида занятий рейтинговая система оценки дается 0.3 балла (максимально 50 занятий (Л+Пз+Лр+КСР) * 0,3 балла = 15 баллов).

№ п/п	Модуль, раздел (в соответствии с РП)	Контролируемые компетенции (или их части)	Вид оценочного средства
1	Раздел 1	ОПК-3	Устный контроль
2	Раздел 2	ОПК-3	Устный контроль, отчет по лабораторным работам
3	Раздел 3	ОПК-3	Устный контроль, отчет по лабораторным работам

Назначение устного контроля - мониторинг эффективности теоретической подготовки студентов к выполнению практических работ, а также эффективности их подготовки в рамках самостоятельной работы.

Параметры оценочного средства для устного контроля.

Устный контрольный опрос состоит из 1-2 устных вопросов. За каждый правильный ответ студентам начисляется до 2 баллов, в зависимости от степени развернутости ответа. Максимальное количество баллов за семестр, которое может получить студент за результаты устного контрольного опроса – 20. Примерные списки вопросов для устного контроля представлены в приложении 1 к рабочей программе дисциплины.

В ходе практических и лабораторных занятий студенты изучают и настраивают программно-аппаратные средства обеспечения информационной безопасности информационных сетей. Максимальное количество баллов за семестр, которое может получить студент по результатам устного контроля выполнения практических заданий – 16 (8 практических работ * 2 балла).

Параметры оценочного средства для устного отчета по выполнению практических заданий по изучению программно-аппаратных средств обеспечения информационной безопасности

Критерии оценки	баллы		
	2 балла	1 балл	0 баллов
Выполнение заданий	Полностью и корректно выполнены все задания. В ходе устного отчета показывает понимание задач и результатов практической работы.	Не полностью выполнены задания, допущены одна – две ошибки. В ходе устного отчета показывает понимание задач и результатов практической работы, но испытывает затруднения с выводами. В ходе устного отчета выказывает ошибки и поверхностные суждения о задачах и результатах практической работы.	Задание не выполнены или задание выполнено не полностью и допущено более 3-х ошибок. С трудом формулирует свои мысли о задачах и результатах практической работы.

Возможны «премиальные» баллы (до 15), которые могут быть добавлены студенту за активные формы работы, высокое качество выполненных практических работ и т.д.

Максимальное количество баллов за текущую работу в семестре ограничивается 96 баллами.

Промежуточная аттестация проводится в форме зачета. В течение семестра за выполнение заданий текущего контроля студенту начисляются баллы и в конце семестра суммируется для вычисления итогового рейтинга студента. В случае, если студент набирает необходимый минимум баллов (40 баллов, из них за выполнение практических заданий – не менее 25), зачет ставится автоматически.

Пример тестовых заданий для проверки сформированности компетенции ОПК-3:

1) Какова длина хеш-строки в символах, рассчитанной по алгоритму хеширования SHA1? (20, 30, 40, 50)

2) Как называется механизм сетей TCP/IP, позволяющий преобразовывать IP-адреса транзитных пакетов? (NAT, VLAN, DNS, UDP)

3) Как называется протокол туннелирования сетевых пакетов, инкапсулирующий пакеты сетевого уровня модели OSI в IP-пакеты? (VPN, PPTP, PPP, GRE)

4) Как называется технология защиты от сетевых атак, проверяющая входящий траффик на корректность? (SPI, FTP, DNS, PPTP)

5) Как называется идентификатор беспроводной локальной сети? (ID, LID, SID, SSID)

6) Что из перечисленного НЕ является алгоритмом шифрования? (MD4, RC4, AES, DES)

7) Сколько протоколов входит в набор стандартов IPSec? (1, 2, 3, 4)

8) Как называется намеренно созданный дефект в алгоритме программы, позволяющий в дальнейшем получить несанкционированный доступ к этой программе или ее данным? (Exploit, Troyan, Rootkit, Backdoor)

Разработчик: доцент, Безлер И.В.

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю подготовки **09.03.02 Информационные системы и технологии**.

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники
«08» апреля 2024 г. протокол № 8

И.О. зав. кафедрой _____ Колесник С.Н.