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.
«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля**) Б1.В.ДВ.03.01 Комплексная система защиты информации**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

Направленность (профиль) подготовки направленность (профиль) N 7 "Техническая защита информации"

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета
Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:
Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

Цели и задачи дисциплины 10.03.01 **«Информационная безопасность»** направленность (профиль) "Техническая защита информации",

Цели: Главной целью дисциплины является формирования у обучающихся универсальных, общепрофессиональных и профессиональных компетенций в соответствии с требованиями ФГОС ВО 10.03.01 «Информационная безопасность» направленность (профиль) "Техническая защита информации", а также изучение теоретических, методологических и практических проблем комплексного обеспечение информационной безопасности автоматизированных систем, формирования, функционирования и развития систем управления информационной безопасностью и комплексной защитой информации

Задачи:

– практико-ориентированное обучение, позволяющее сочетать фундаментальные знания с практическими навыками по направлению подготовки 10.03.01 Информационная безопасности, учитывающие требования предъявляемых к выпускникам на рынке труда, обобщения отечественного и зарубежного опыта, проведения консультаций с ведущими работодателями и иных источников;

– формирование готовности выпускников Университета к активной профессиональной и социальной деятельности

- раскрытие места информационной безопасности и защиты информации в системе информационных отношений;

- раскрытие направлений и областей деятельности субъектов информационных отношений, составной частью которых является обеспечение информационной безопасности и защита информации;

- определение места защиты информации в обеспечении сохранности документальной базы, раскрывающей различные стороны социально-экономического и культурного развития страны.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «**Комплексная система защиты информации**»:

Для изучения данной учебной дисциплины (модуля) необходимы знания, умения и навыки, формируемые предшествующими дисциплинами*:*

«История», «Психология социального взаимодействия, саморазвития и самоорганизации», «Документоведение. Нормативные документы в сфере информационной безопасности». «Защита и обработка конфиденциальных документов», «Основы построения и функционирования технических средств защиты информации»,

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: «Основы управления информационной безопасностью», «Организационное и правовое обеспечение информационной безопасности», «Государственная итоговая аттестация».

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций: **ПК-11-** способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

Знать: нормативную документацию в сфере защиты информации при решении задач профессиональной деятельности
Уметь: проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов

Владеть: навыками по применению заданной методики, обработке, оценке погрешности и достоверности полученных результатов

ПК-12 способностью принимать участие в проведении экспериментальных исследований системы защиты информации

Знать: нормативную документацию в сфере защиты информации при решении задач профессиональной деятельности
Уметь: принимать участие в проведении экспериментальных исследований системы защиты информации

Владеть: способностью принимать участие в проведении экспериментальных исследований системы защиты информации

ПК-13 способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Знать: нормативную документацию в сфере защиты информации при решении задач профессиональной деятельности
Уметь: принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

Владеть: способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		7			
Аудиторные занятия (всего)	144/4	144/4			
В том числе:	-	-	-	-	-
Лекции	52/1,44	52/1,44			
Практические занятия (ПЗ)	26/0,72	26/0,72			
Семинары (С)					
Лабораторные работы (ЛР)					
КСР	4/0,11	4/0,11			
Самостоятельная работа (всего)	62/1,72	62/1,72			

В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы					
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)					
Общая трудоемкость часы	144	144			
зачетные единицы	4	4			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

Раздел 1. Тема 1 Автоматизированная система

Раздел 2. Тема 2 Нормативно – правовое регулирование деятельности в области защиты информации в РФ

Тема 3 Организационно-технические методы ЗИ

Тема 4 Нормативно-методические документы ФСТЭК России

Тема 5 Выбор методов и способов защиты информации. Методы и способы защиты информации от НСД

Тема 6 Методы и способы защиты информации от утечки по ТКУИ

Тема 7 Основные вопросы управления обеспечением безопасности

Тема 8 Создание системы защиты конфиденциальной информации (КИ)

Предпроектное обследование СЗ (КИ)

Тема 9 Техническое задания на разработку СЗ (КИ)

Структура информационной системы

Наличие подключений к сетям связи общего пользования и (или) сетям международного информационного обмена

Раздел 3. Тема 10. Угрозы несанкционированного доступа к информации

Тема 11. Угрозы доступа в операционную среду компьютера с использованием штатного программного обеспечения

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств

Угрозы создания нештатных режимов работы программных (программно-аппаратных) средств.

Тема 12. Угрозы внедрения вредоносных программ (программно - математического воздействия).

• преднамеренных изменений служебных данных;

• игнорирования предусмотренных в штатных условиях ограничений на состав и характеристики обрабатываемой информации;

• искажения (модификации) самих данных и т.п.;

Тема 13. Угрозы НСД реализуемые с использованием протоколов сетевого осуществляются с использованием взаимодействия программных и программно-аппаратных средств ввода/вывода компьютера

Источники угроз НСД:

-нарушитель;

-носитель вредоносной программы;

-аппаратная закладка

Внешние источники угроз:

-разведывательные службы государств;

-криминальные структуры;

-конкуренты (конкурирующие организации);

-недобросовестные партнеры;

-внешние субъекты (физические лица)

Внутренние источники угроз.

Категории внутренних нарушителей

Источники угроз НСД в ИС(КИ)

-нарушитель

-носитель вредоносной программы

-аппаратная закладка

-аппаратный элемент компьютера

-программный контейнер

Тема 14. Уязвимости ИС(КИ)

-уязвимости системного программного обеспечения (в том числе протоколов сетевого взаимодействия);

-уязвимости прикладного программного обеспечения (в том числе средств защиты информации).

Характеристика угроз непосредственного доступа в операционную среду.

Классификация угроз по условиям реализации

Тема 15. Характеристика угроз программно-математических воздействий и

нетрадиционных информационных каналов.

Вредоносные программы.

Тема 16. Нетрадиционные информационные каналы.

Общая характеристика результатов НСД:

-нарушение конфиденциальности;

-нарушению целостности (уничтожение, изменение);

-нарушению доступности (блокирование)

Тема 17. Угрозы из внешних сетей:

-«Анализа сетевого трафика» с перехватом передаваемой по сети информации;

-сканирование сети, выявление открытых портов и служб, открытых соединений и др.;

-внедрение ложного объекта сети;

-подмена доверенного объекта;

-выявление паролей;

-получения НСД путем подмены доверенного объекта;

-«Отказ в обслуживании»;

-навязывание ложного маршрута путем несанкционированного изменения маршрутно-адресных данных;

-удаленный запуск приложений;

-внедрение по сети вредоносных программ

Раздел 4.Тема 18. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. ГОСТ Р 51275-2006

Субъективные факторы

Объективные факторы

Виды защиты информации

Правовая защита информации

Техническая защита информации

Криптографическая защита информации

Физическая защита информации

Раздел 5. Тема 19. ОСОБЕННОСТИ РАБОТЫ С ПЕРСОНАЛОМ, ВЛАДЕЮЩИМ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

Персонал - основная опасность утраты конфиденциальной информации

Организационные мероприятия по работе с персоналом, полу¬чающим доступ к конфиденциальной информации

Методы получения ценной информации у персонала

От персонала информация легко переходит к злоумышленнику по причине:

Ошибочные и безответственные действия персонала

Особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией.

Подготовительные этапы процесса приема сотрудника на работу.

Поиску кандидата на вновь создаваемую или вакантную долж¬ность - системный характер.

Основные на¬правления поиска кандидата

Технологическая цепочка приема сотрудников, работа которых связана с владением конфиденциальной информацией, включает следующие процедуры

Личные Качества, которыми должен обладать потенциальный сотрудник. Личные качества, не способствующие сохранению секретов

Доступ персонала к конфиденциальным сведениям, документам и базам данных

Текущая работа с персоналом, обладающим конфиденциальной информацией. Задачи обучения включают в себя изучение. Методика обучения.

Основными формами контроля качества работы персонала, повышения ими своих профессиональных знаний, в том числе в ча-сти защиты информации,

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Техническая защита информации	1-19
2	Радиотехнические цепи и сигналы	1-19
3	Защита информации от несанкционированного доступа	1-19
4	Электроника и схемотехника	1-19
5	Операционные системы	1-19
6	Базы данных	1-19
7	Электротехника	1-19
8	Основы построения и функционирования специальных технических средств	1-19
9	Безопасность компьютерных сетей	1-19
10	Практика по получению первичных профессиональных умений и навыков	1-19
11	Эксплуатационная практика	1-19

12	Проектно-технологическая практика	1-19

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1	2	1			3	6
2.	***Раздел 2***	Тема 2	2	1			3	6
3.	***Раздел 2***	Тема 3	2	1			3	6
4.	***Раздел 2***	Тема 4	2	1			3	6
5.	***Раздел 2***	Тема 5	2	1			3	6
6	***Раздел 2***	Тема 6	2	1			3	6
7	***Раздел 2***	Тема 7	2	1			4	7
8.	***Раздел 2***	Тема 8	2	1			3	6
9.	***Раздел 2***	Тема 9	2	2			3	7
10	***Раздел 3***	Тема 10	2	2			3	7
11	***Раздел 3***	Тема 11	2	2			4	8
12	***Раздел 3***	Тема 12	2	2			3	7
13	***Раздел 3***	Тема 13	4	2			3	7
14	***Раздел 3***	Тема 14	4	2			3	7
15	***Раздел 3***	Тема 15	4	2			3	7
16	***Раздел 3***	Тема 16	4	1			3	8
17	***Раздел 3***	Тема 17	4	1			4	9
18	***Раздел 4***	Тема 18	4	1			4	9
19	***Раздел 4***	Тема 19	4	1			4	9

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 2***	Практич. Занятие№1	4	Тестовый контроль по теме	ПК-10
2.	***Раздел 2***	Практич. Занятие№2	6	Тестовый контроль по теме	ПК-10

3.	***Раздел 2***	Практич. Занятие№3	4	Тестовый контроль по теме	ПК-11
4.	***Раздел 2***	Практич. Занятие№4	4	Тестовый контроль по теме	ПК-11
5.	***Раздел 3***	Практич. Занятие№5	2	Тестовый контроль по теме	ПК-12
6.	***Раздел 3***	Практич. Занятие №6	4	Тестовый контроль по теме	ПК-12
	Раздел 4	Практич. Занятие №7	2	Тестовый контроль по теме	ПК-12

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-6**	Подготовка к практич. работе №1	№1	Учебный сайт	36
8		Практическая работа №1.		Учебный сайт	
9		Подведение итогов по практич. работе №1. Работа над ошибками по контрольной работе №1.		Учебный сайт	
10-16	**9-19**	Подготовка итоговой экзаменационной работы	№2	Учебный сайт	26
17		Подготовка доклада с презентацией		Учебный сайт	
18		Подведение итогов		Учебный сайт	

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Комплексная система защиты информации». Нормативные документы технической защиты информации», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- выполнение индивидуальных проектов;
- подготовка к контрольным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Основы управления информационной безопасностью». направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

1 Краковский Ю. М Информационная безопасность и защита информации: учебное пособие Иркутск: ИрГУПС, 2016 50

2.Прохорова О.В. Информационная безопасность и защита информации: Учебник [Электронный ресурс]
//biblioclub.ru/index.php?page=book&id=438331 Самара: СГА-СУ, 2014 100% Онлайн

б) дополнительная литература

1. Нортон, П. Персональный компьютер [Текст]. Кн. 1. Аппаратно-программная организация ; Кн. 2. Модернизация и ремонт / П. Нортон, Дж. Гудман. - СПб. : BNY, 1999. - 848 ил
2. Попов, В. Б. Основы информационных и телекоммуникационных технологий [Текст] : учеб. пособие. Ч. 1. Программно-аппаратное обеспечение / В.Б. Попов. - М. : Финансы и статистика, 2005. - 144 с.

в) программное обеспечение

Система тестирования и анализа аппаратной платформы ЭВМ.

г) базы данных, информационно-справочные и поисковые системы

1. Учебный сайт Лаборатории ТЗИ Физического факультета ИГУ - – Режим доступа: https://sites.google.com/view/ltzi/, свободный.

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине ««Основы управления информационной безопасностью», используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения химических исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем общей и неорганической химии на лекциях, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Входной контроль (25 вариантов, 7-й семестр), представляет собой перечень из 10-15 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 15 минут. Проверяется уровень входных знаний.

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (10 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

11.3. Оценочные средства для промежуточной аттестации

(в форме зачета).

Тестовые работы (10 комплектов по 3-5 вариантов). Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

доцент  Н.И.Глухов

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой  Колесник С.Н.