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 **Б1.Б.25 Основы информационной безопасности**

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

1. Цели и задачи дисциплины (модуля)

Целью курса «Основы информационной безопасности» раскрытие сущности и значения информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристика составляющих информационной безопасности и защиты информации в системе экономической безопасности организации.

В состав задач изучения дисциплины входят:

- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий и методологических принципов создания систем защиты информации в системе безопасности организации;
- изучение видов защищаемой информации, угроз информационной безопасности, методов и средств обеспечения информационной безопасности, механизмов защиты информации, моделей безопасности, критериев оценки защищенности и обеспечения безопасности информационных систем.

2. Место дисциплины в структуре ОПОП

Учебная дисциплина «Основы информационной безопасности» входит в обязательную часть дисциплин.

В структуре ОПОП дисциплина входит в обязательную часть программы.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

ОК-5 способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики. В результате изучения дисциплины студент должен:

Знать: методологические и организационные основы обеспечения информационной безопасности и защиты интересов личности, общества, государства, а также нормы профессиональной этики.

Уметь: понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики:

Владеть: навыками административно-управленческой деятельности для формирования

комплекса мер по информационной безопасности хозяйствующих субъектов

ОПК-4 - способностью понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации.

В результате изучения дисциплины студент должен:

Знать: нормативно правовые и методические документы по защите информации, классификацию и характеристики составляющих информационной безопасности;

Уметь: понимать значение информации в развитии современного общества, определять требования по обеспечению информационной безопасности;

Владеть: навыками применения информационных технологий для поиска и обработки информации с целю обеспечения защиты информации.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		1			
Аудиторные занятия (всего)	84/2,3	84/2,3			
В том числе:	-	-	-	-	-
Лекции	36/1,0	36/1,0			
Практические занятия (ПЗ)					
Семинары (С)					
Лабораторные работы (ЛР)	18/0,5	18/0,5			
КСР	-	-			
Самостоятельная работа (всего)	54/1.5	54/1.7			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	54/1.5	54/1.5			
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	54/1,5	54/1,5			
Общая трудоемкость часы	108	108			
зачетные единицы	3	3			

5. Содержание дисциплины (модуля)

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

нумеруются

Т 1. Введение. Сущность и понятие информационной безопасности. Значение информационной безопасности и ее место в системе национальной безопасности. Современная Доктрина информационной безопасности Российской Федерации. Сущность и понятие защиты информации.

Т 2. Цели и значение защиты информации

Т4. Теоретические и концептуальные основы защиты информации

Т5. Организационные основы и методологические принципы защиты информации

Т6. Современные факторы, влияющие на защиту информации

Т7. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности

Т8. Критерии, условия и принципы отнесения информации к защищаемой

Т9. Понятие и структура угроз защищаемой информации

Т10. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию

Т11. Причины, обстоятельства и условия дестабилизирующего воздействия на защищаемую информацию

Т12. Каналы и методы несанкционированного доступа к конфиденциальной информации

Т13. Направления, виды и особенности деятельности разведывательных служб по несанкционированному доступу к конфиденциальной информации

Т14.Объекты 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	Б1. Б.16 Информатика	1-14
2	Б1. Б.30 Документоведение. Нормативные документы технической защиты информации	1-14
3	Б1.Б.29 Безопасность систем баз данных	1-14
4	Б2.В.01(У) Практика по получению первичных профессиональных умений и навыков в сфере технической защиты информации	1-14

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	4			1	2	7

2.	***Раздел 2***	Тема 2	4			1	4	9
3.	***Раздел 3***	Тема 3	2			1	4	7
4.	***Раздел 4***	Тема 4	2			1	4	7
5.	***Раздел 5***	Тема 5	2			1	4	7
6.	***Раздел 6***	Тема 6	2			1	4	7
7.	***Раздел 7***	Тема 7	2			1	4	7
8.	***Раздел 8***	Тема 8	2			1	4	7
9.	***Раздел 9***	Тема 9	2			2	4	8
10.	***Раздел 10***	Тема 10	4			2	4	10
11.	***Раздел 11***	Тема 11	4			2	4	10
12.	***Раздел 12***	Тема 12	2			2	4	8
13.	***Раздел 13***	Тема 13	2			1	4	7
14	***Раздел 14***	Тема 14	2			1	4	7

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 1***	Лабораторная №1	1	Тестовый контроль по теме	ОК-5 ОПК-4
2.	***Раздел 2***	Лабораторная №2	1	Тестовый контроль по теме	ОК-5 ОПК-4
3.	***Раздел 3***	Лабораторная №3	1	Тестовый контроль по теме	ОК-5 ОПК-4
4.	***Раздел 4***	Лабораторная №4	1	Тестовый контроль по теме	ОК-5 ОПК-4
5.	***Раздел 5***	Лабораторная №5	1	Тестовый контроль по теме	ОК-5 ОПК-4
6.	***Раздел 6***	Лабораторная №6	1	Тестовый контроль по теме	ОК-5 ОПК-4
7.	***Раздел 7***	Лабораторная №7	1	Тестовый контроль по теме	ОК-5 ОПК-4
8.	***Раздел 8***	Лабораторная №8	1	Тестовый контроль	ОК-5

				по теме	ОПК-4
9.	***Раздел 9***	Лабораторная №9	2	Тестовый контроль по теме	ОК-5 ОПК-4
10.	***Раздел 10***	Лабораторная №10	2	Тестовый контроль по теме	ОК-5 ОПК-4
11.	***Раздел 11***	Лабораторная №11	2	Тестовый контроль по теме	ОК-5 ОПК-4
12.	***Раздел 12***	Лабораторная №12	2	Тестовый контроль по теме	ОК-5 ОПК-4
13.	***Раздел 13***	Лабораторная №13	1	Тестовый контроль по теме	ОК-5 ОПК-4
14.	***Раздел 14***	Лабораторная №14	1	Тестовый контроль по теме	ОК-5 ОПК-4

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-7**	Подготовка к контрольной работе	№1	Учебный сайт	30
8		Контрольная работа		Учебный сайт	
9		Подведение итогов по контрольной работе. Работа над ошибками по контрольной работе.		Учебный сайт	
10-16	**8-14**	Подготовка итоговой зачетной работы	№2	Учебный сайт	24
17		Подготовка доклада с презентацией		Учебный сайт	

6.2. Методические указания по организации самостоятельной работы студентов

Самостоятельная работа студентов – индивидуальная учебная деятельность, осуществляемая без непосредственного руководства преподавателя, в ходе которой студент

активно воспринимает, осмысливает полученную информацию, решает теоретические и практические задачи. 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).

В процессе проведения самостоятельной работы формируется компетенция ОК-5;

ОПК-4. Контроль самостоятельной работы на лабораторных занятиях и на КСР, по окончании соответствующих тем.

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. Ю.Н. Загинайлов Теория информационной безопасности и методология защиты информации: учебное пособие [Электронный ресурс] //biblioclub.ru/index.php? page=book&id=276557 М.; Берлин: Директ-Медиа, 2015 100% онлайн.
2. С.А. Нестеров Основы информационной безопасности: Учебное пособие [Электронный ресурс] //biblioclub.ru/index.php? page=book&id=363040 СПб.: Политехнический университет, 2014 100% онлайн.

б) 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 и лекционная аудитория, 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.

Программное обеспечение:

1. 1. M Microsoft Access 2019, Microsoft SQL Server, Oracle Server

10. Образовательные технологии

Для достижения планируемых результатов обучения, при изучении дисциплины «Основы информационной безопасности» 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 (6 вариантов, 1-й семестр), представляет собой перечень из 10 вопросов и заданий. Входной контроль проводится в письменном виде на первом лабораторном занятии в течение 15 минут. Проверяется уровень входных знаний.

11.2. Оценочные средства текущего контроля

Текущий контроль осуществляется за счет контроля решенных задач на лабораторных занятиях, а также решения задач на лекционных занятиях, в том числе у доски.

В конце каждой темы, на последнем лабораторном занятии студенты выполняют специальное задание, с написанием отчета. Данное задание предназначено для проверки усвоения теоретического материала, а также навыков выполнения практических и творческих задач, связанных с разработкой программного обеспечения и работы с различными БД и СУБД. Таким образом, в течение курса студенты должны выполнить 10 спецзаданий, и получить оценку за задание и отчет по нему.

За выполнение каждого специального задания студент может набрать максимум 10 баллов. Баллы, за каждое из выполненных спецзаданий заносятся в индивидуальный семестровый рейтинг студента, и используются при проведении промежуточной аттестации по дисциплине. При наборе менее 5 баллов спецзадание считается не выполненным.

Кол-во баллов	Критерии оценивания	Оценка за спецзадание
5-6	Цели задания усвоены полностью, формулировки корректны и точны. Практическое задание выполнено, но допущены ошибки, не носящие критический характер. В отчете присутствуют серьезные ошибки, структура отчета недостаточно проработана, не все факторы отражены.	«удовлетворительно»

	При этом цели и задачи в общем достигнуты и отражены в отчете.	
7-8	Цели задания усвоены полностью, формулировки корректны и точны. Практическая часть выполнена полностью, без серьезных ошибок и замечаний, все цели и задачи выполнены и реализованы. В отчете отражены все основные моменты выполнения спецзадания, но могут присутствовать небольшие неточности и ошибки в изложении фактов.	«хорошо»
9-10	Цели задания усвоены полностью, формулировки корректны и точны. Практическая часть выполнена полностью, без ошибок и замечаний, все цели и задачи выполнены и реализованы. В отчете отражены все основные моменты выполнения спецзадания, структура отчета логична и последовательна, отсутствуют ошибки оформления и изложения всех аспектов выполненной работы.	«отлично»

ТЕСТОВЫЕ ВОПРОСЫ ПО ДИСЦИПЛИНЕ

Б1. Б.25 Основы информационной безопасности

КОМПЕТЕНЦИИ ОК-5; ОПК-4

Вариант 1

1. Определение термина «информация»:
А - совокупность содержащихся в базах данных сведений;
Б - сведения (сообщения, данные) независимо от формы их представления.
В - сведения (сообщения, данные) воспроизводимые различными системами.
2. Определение термина «обладатель информации»:
А - лицо, самостоятельно создавшее информацию;
Б - лицо, получившее на основании закона или договора право разрешать или ограничивать доступ к информации;

В - лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам.
3. Технические способы защиты информации в зависимости от используемых средств классифицируются как:
А - полуактивные;
Б - пассивные;
В – разноплановые.
4. Указать меры, которые устанавливаются для обеспечения правового режима защиты персональных данных;
5. Указать источники права в области оборота сведений составляющих коммерческую тайну;
6. Если сведения относятся к государственной тайне проанализировать порядок установления степени их секретности.
7. Пассивные способы защиты информации:
А - создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств;
Б - ослабление наводок ПЭМИ в посторонних проводниках и соединительных линиях технических средств, выходящих за пределы контролируемой зоны;
В - создание маскирующих электромагнитных помех в цепях заземления.
8. Несанкционированный доступ к информации»:
А - доступ, реализующий возможности совокупности физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация;
Б - доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств;
В - доступ с использованием совокупности средств технической разведки и прочих средств, которыми добывается защищаемая информация.
9. Предоставление информации -
А - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;
Б - действия, направленные на распространение сведений в средствах массовой информации;
В - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц.
10. Построить схему реализации угрозы информационной безопасности в атаку.
11. Защита информации представляет собой принятие мер, перечислить.
12. Исходя из требований № 149-ФЗ защиту информации можно разделить так же на несколько уровней:
13. Свойства безопасности информации, перечислить.
14. Способы и методы защиты электронного документооборота, назвать.
15. Риск информационной безопасности:
А – потенциальная возможность использования уязвимостей активов конкретной угрозой для причинения ущерба организации.
Б – потенциальная возможность нанесения ущерба в результате действия угроз информационной безопасности;
В – возможность реализации угрозы информационной безопасности;
Г – неудовлетворительное состояние системы защиты информации.

Вариант 2

1. Перечень объектов информатизации, на которые распространяется требования по аттестации:
   А. Значимых объектов критической информационной инфраструктуры Российской Федерации;

Б. Информационных систем персональных данных (за исключением государственных, муниципальных информационных систем персональных данных);

С. Автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Д. Помещений, предназначенных для ведения конфиденциальных переговоров (далее - защищаемые помещения)

2. Аттестация объектов информатизации –определение.
А. Комплекс организационно-технических мероприятий, результатом которого является документ «Аттестат соответствия», подтверждающий выполнение на объекте информатизации норм и правил, определенных действующим законодательством Российской Федерации.
Б. Проведение комплекса организационных и технических мероприятий и работ по защите информации.
С. Проверка уровня защиты информации на объекте информатизации.
Д. Оценка уровня защиты информации включая эффективность технических и программно-технических средств защиты.
2. Условия обязательной аттестация объектов информатизации.
А. Государственных и муниципальных информационных систем, в том числе государственных, муниципальных информационных систем персональных данных.

Б. Информационных систем управления производством, используемых организациями оборонно-промышленного комплекса, в том числе автоматизированных систем станков с числовым программным управлением.

С. Значимых объектов критической информационной инфраструктуры Российской Федерации.

Д. Помещений, предназначенных для ведения конфиденциальных переговоров.

4. Цели проведения аттестации объекта информатизации
А. Оценка уровня защиты объекта информатизации.

Б. Оценка соответствия внедренного комплекса мер по защите информации и установленных на объекте информатизации средств защиты информации требуемому уровню защищенности информации.

С. Получения лицензии организации для осуществления деятельности по защите информации.

Д. Оценка текущего состояния средств защиты информации по противодействию угроз.

5. В ходе аттестационных испытаний объекта информатизации владельцем объекта информатизации могут вноситься изменения в объект информатизации.
А. Да.

Б. Нет.

С. Да, только в случае наличия необходимой документации на объекте.

Д. По согласованию с федеральным органом исполнительной власти в области защиты информации.

6. Состав разделов программы и методики аттестационных испытаний.
А. Общие положения;
Б. Перечень необходимых документов

С. Программа аттестационных испытаний объекта информатизации

Д. Методики аттестационных испытаний объекта информатизации

7. Перечень мероприятий аттестационных испытаний.
А. Обследование объекта информатизации на предмет оценки соответствия объекта информатизации и условий его эксплуатации требованиям по защите информации, а также документам, предусмотренным пунктом 11 настоящего Порядка;

Б. Проверку наличия у владельца объекта информатизации работников, ответственных за обеспечение защиты информации в ходе эксплуатации объекта информатизации

С. Оценку соответствия принятых на объекте информатизации организационных мер требованиям по защите информации и их достаточности для защиты от актуальных для объекта информатизации угроз безопасности информации;

Д. Оценку эффективности защиты (защищенности) информации от утечки по техническим каналам (только для защищаемых помещений).

8. Аттестация объекта информатизации проводится:
А. На этапе смены собственника объекта информатизации.

Б. На этапе эксплуатации.

С. На этапе создания или развития (модернизации)

Д. На этапе создания.

9. Аттестат соответствия выдается на срок:
А. 5 лет.

Б. 3 года.

С. На весь эксплуатации объекта информатизации.

Д. 2 года.

10. Условия приостановки действия аттестата соответствия.
А. Установления факта несоответствия аттестованного объекта информатизации требованиям по защите информации, в результате чего имеется или имелась возможность возникновения угроз безопасности информации.

Б. Не устранения недостатков, выявленных ФСТЭК России (территориальным органом ФСТЭК России) в соответствии с пунктом 30 настоящего Порядка.

С. Непредставления протоколов контроля уровня защиты информации на аттестованном объекте информатизации.

Д. Обращения владельца объекта информатизации о приостановлении действия аттестата соответствия.

11. Условия прекращения действия аттестата соответствия.
А. Непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок материалов, подтверждающих устранение недостатков.

Б. Непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок протоколов контроля уровня защищенности информации на аттестованном объекте информатизации;

С. Непредставления владельцем объекта информатизации в установленный в уведомлении о приостановлении действия аттестата соответствия срок материалов, подтверждающих проведение аттестации объекта информатизации для измененной архитектуры системы защиты информации;

Д. Обращения владельца объекта информатизации о прекращении действия аттестата соответствия.

12. Действие аттестата соответствия может быть приостановлено на срок:
А. Не более 30 календарных дней.

Б. Не более 10 календарных дней.

С. Не более 90 календарных дней.

Д. Не более 3х календарных дней.

13. Функции ФСТЭК при аттестации объекта информатизации.
А. Орган по аттестации объектов информатизации.

Б. Федеральный орган исполнительной власти

С. Орган местного самоуправления.

Д. Надзорный орган.

14. Решение о прекращении действия аттестата соответствия оформляется:
А. Приказом руководителя субъекта информатизации.

Б. Приказом ФСТЭК России (территориального органа ФСТЭК России).

С. Решением суда.

Д. Приказом вышестоящей организации субъекта информатизации.

- Обновления

11.3. Оценочные средства для промежуточной аттестации

Промежуточная аттестация проводится в форме зачета.

Примерные вопросы к зачету

1. Структура государственной системы защиты информации (схема).
2. Система документации по технической защите информации (схема).
3. Действующие документы по защите информации с учетом категорий доступа к ней и видов информационных систем.
4. Определение информационной безопасности.
5. Определение защиты информации.
6. Меры по обеспечению информационной безопасности.
7. Основные организационно-технические мероприятиям по защите информации.
8. Источники угрозы информационной безопасности.
9. Угрозы информационной безопасности.
10. Уязвимости информационной безопасности.
11. Атаки информационной безопасности.
12. Построить логическую цепочку реализации угрозы информационной безопасности.
13. Построить схему классификации источников угроз ИБ.
14. Объективные уязвимости.
15. Субъективные уязвимости.
16. Случайные уязвимости.
17. Понятие лицензии (пользовательская лицензия).
18. Определение лицензионной политики.
19. Понятие коммерческой лицензии.
20. Понятие открытой лицензии.
21. Гарантируемые права открытой лицензии.
22. Понятие нелицензионного программного обеспечения.
23. Угрозы при использовании нелицензионного программного обеспечения.
24. Закон, определяющий правовые основы информационной безопасности (наименование, когда принят, основные требования).

Разработчик:

Доцент кафедры РФиРЭ _____ Серёдкин С.П.

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ОПОП по направлению и профилю подготовки **10.03.01 Информационная безопасность.**

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

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