МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
"САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ"

Кафедра № 33

УТВЕРЖДАЮ
Руководитель образовательной программы

доц.,к.э.н.,доц.
(должность, уч. степень, звание)

Т.Н. Елина
(инициалы, фамилия)

(подпись)
«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Основы информационной безопасности»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.03.01
Наименование направления подготовки/ специальности	Информационная безопасность
Наименование направленности/ специализации	Безопасность компьютерных систем
Форма обучения	очная
Год приема	2026

Санкт-Петербург– 2026

Лист согласования рабочей программы дисциплины

Программу составил (а)

доц.,к.т.н.,доц. — 20.02.26 — В.А. Рындюк
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Программа одобрена на заседании кафедры № 33
«20» февраля 2026 г, протокол № 7

Заведующий кафедрой № 33

д.т.н.,проф. — 20.02.26 — С.В. Беззатеев
(уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Заместитель директора института №3 по методической работе

доц.,к.т.н. — 20.02.26 — Н.В. Решетникова
(должность, уч. степень, звание) (подпись, дата) (инициалы, фамилия)

Аннотация

Дисциплина «Основы информационной безопасности» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.03.01 «Информационная безопасность» направленности/специализации «Безопасность компьютерных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ОПК-1 «Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства»

ОПК-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности»

ОПК-8 «Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности»

ОПК-12 «Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений»

Содержание дисциплины охватывает круг вопросов, раскрывающих сущность и значение информационной безопасности и защиты информации, их места в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности

Преподавание дисциплины предусматривает следующие формы организации учебного процесса: лекции, лабораторные работы, самостоятельная работа студента, консультации.

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме зачета (4 семестр).

Общая трудоемкость освоения дисциплины составляет 2 зачетных единицы, 72 часа.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Дисциплина имеет своей целью: обеспечить выполнение требований, изложенных в федеральном государственном образовательном стандарте высшего профессионального образования.

Изучение дисциплины направлено на формирование перечисленных ниже элементов компетенций.

Целью освоения дисциплины «Основы информационной безопасности» является раскрытие сущности и значения информационной безопасности и защиты информации, ее место в системе национальной безопасности, определение теоретических, концептуальных, методологических и организационных основ обеспечения безопасности информации, классификация и характеристики составляющих информационной безопасности и защиты информации, установление взаимосвязи и логической организации входящих в них компонентов, получение обучающимися необходимых знаний, умений и навыков в области развития методов и средств защиты информаци.

1.2. Дисциплина входит в состав обязательной части образовательной программы высшего образования (далее – ОП ВО).

1.3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ОП ВО.

В результате изучения дисциплины обучающийся должен обладать следующими компетенциями или их частями. Компетенции и индикаторы их достижения приведены в таблице 1.

Таблица 1 – Перечень компетенций и индикаторов их достижения

Категория (группа) компетенции	Код и наименование компетенции	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции	ОПК-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ОПК-1.З.1 знает понятия информации и информационной безопасности ОПК-1.З.2 знает место и роль информационной безопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики ОПК-1.З.3 знает источники и классификацию угроз информационной безопасности ОПК-1.У.1 умеет классифицировать и оценивать угрозы информационной безопасности ОПК-1.В.1 владеет навыками оценки и анализа необходимости внедрения средств информационной безопасности в процессы производства
Общепрофессиональные компетенции	ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по	ОПК-5.В.1 владеет навыками работы с нормативными документами, государственными и международными стандартами в области информационной безопасности и защиты информации

	защите информации в сфере профессиональной деятельности	
Общепрофессиональные компетенции	ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.З.1 знает принципы и порядок работы информационно-справочных систем
Общепрофессиональные компетенции	ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	ОПК-12.З.1 знает принципы формирования политики информационной безопасности в информационных системах

2. Место дисциплины в структуре ОП

Дисциплина может базироваться на знаниях, ранее приобретенных обучающимися при изучении следующих дисциплин:

- «Информатика»;
- «Математическая логика и теория алгоритмов».

Знания, полученные при изучении материала данной дисциплины, имеют как самостоятельное значение, так и могут использоваться при изучении других дисциплин:

- «Техническая защита информации;
- «Защита информационных процессов в компьютерных системах».

3. Объем и трудоемкость дисциплины

Данные об общем объеме дисциплины, трудоемкости отдельных видов учебной работы по дисциплине (и распределение этой трудоемкости по семестрам) представлены в таблице 2.

Таблица 2 – Объем и трудоемкость дисциплины

Вид учебной работы	Всего	Трудоемкость по семестрам
		№4
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	2/ 72	2/ 72

Из них часов практической подготовки		
Аудиторные занятия, всего час.	34	34
в том числе:		
лекции (Л), (час)	17	17
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	17	17
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)		
Самостоятельная работа, всего (час)	38	38
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Зачет	Зачет

4. Содержание дисциплины

4.1. Распределение трудоемкости дисциплины по разделам и видам занятий.

Разделы, темы дисциплины и их трудоемкость приведены в таблице 3.

Таблица 3 – Разделы, темы дисциплины, их трудоемкость

Разделы, темы дисциплины	Лекции (час)	ПЗ (СЗ) (час)	ЛР (час)	КП/КР (час)	СР (час)
Семестр 4					
Раздел 1. Введение. Сущность и понятие информационной безопасности	2				4
Раздел 2. Значение информационной безопасности и ее место в системе национальной безопасности	2		2		4
Раздел 3. Состав и классификация защищаемой информации	2		2		4
Раздел 4. Теория защиты информации (ТЗИ). Методологический базис ТЗИ.	4		4		4
Текущий контроль			1		6
Раздел 5. Понятие и структура угроз защищаемой информации	2		2		6
Раздел 6. Классификация методов и средств защиты информации	2		2		4
Раздел 7. Система защиты информации.	3		4		6
Итого в семестре:	17		17		38
Итого	17	0	17	0	38

Практическая подготовка заключается в непосредственном выполнении обучающимися определенных трудовых функций, связанных с будущей профессиональной деятельностью.

4.2. Содержание разделов и тем лекционных занятий.

Содержание разделов и тем лекционных занятий приведено в таблице 4.

Таблица 4 – Содержание разделов и тем лекционного цикла

Номер раздела	Название и содержание разделов и тем лекционных занятий

1	*Раздел 1. Введение. Сущность и понятие информационной безопасности* Предмет и задачи курса. Значение и место курса в, подготовке специалистов, по защите информации. Научная и учебная взаимосвязь курса с другими дисциплинами. Становление и развитие понятия "информационная безопасность" (ИБ). Современные подходы к определению понятия. Сущность информационной безопасности. Связь информационной безопасности с информатизацией общества. Структура информационной безопасности. Определение понятия информационная безопасность", основные характеристики ИБ.
2	*Раздел 2. Значение информационной безопасности и ее место в системе национальной безопасности* Значение информационной, безопасности для субъектов информационных отношений. Понятие и современная концепция национальной безопасности РФ. Место информационной безопасности в системе национальной безопасности РФ. Политика ИБ. Законодательство в области информационной безопасности. Принципы формирования политики информационной безопасности в организации/на предприятии. Информационно-справочные системы.
3	*Раздел 3. Состав и классификация защищаемой информации* Принципы отнесения информации к защищаемой. Понятие конфиденциальной информации. Виды тайн. Государственная тайна. Режимы секретности. Профессиональные тайны. Коммерческая тайна. Персональные данные. Принципы отнесения информации к определенному виду тайны. Законодательная защита. Хранение тайны и наказание за ее разглашение.
4	*Раздел 4. Теория защиты информации (ТЗИ). Методологический базис ТЗИ.* Существующие подходы к содержательной части понятия "защита информации" и способы реализации содержательной части Методологическая основа раскрытия сущности и определения понятия защиты информации. Формы выражения нарушения статуса информации Обусловленность статуса информации ее уязвимостью. Теории нестрогой математики, нечетких множеств, неформального оценивания, неформального поиска оптимальных решений.
5	*Раздел 5. Понятие и структура угроз защищаемой информации* Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации. Классификация угроз. Деление угроз по видам природе происхождения, по предпосылкам появления, по источникам. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.
6	*Раздел 6. Классификация методов и средств защиты информации* Понятие методов защиты информации. Их классификация. Методы препятствие, управление доступом, маскировка, регламентация, принуждение и побуждение. Понятие объекта защиты. Виды и способы дестабилизирующего воздействия на объекты защиты. Средства защиты, их связь с методами защиты. Классификация средств ЗИ. Основные средства ЗИ программные, технические, организационные средства. Криптографические средства защиты. Стеганография.
7	*Раздел 7. Системы защиты информации.* Понятие систем защиты информации. Принципы построения СЗИ. Требования к СЗИ. Основы архитектурного построения СЗИ Функциональное и организационное построение СЗИ. Понятия типизации и стандартизации СЗИ, их значение. Классификация СЗИ по активности реагирования и уровню защиты. Уровни типизации и стандартизации Проектирование СЗИ. Современные сертифицированные СЗИ Проектирование СЗИ.

4.3. Практические (семинарские) занятия

Темы практических занятий и их трудоемкость приведены в таблице 5.

Таблица 5 – Практические занятия и их трудоемкость

№ п/п	Темы практических занятий	Формы практических занятий	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Учебным планом не предусмотрено					
Всего					

4.4. Лабораторные занятия

Темы лабораторных занятий и их трудоемкость приведены в таблице 6.

Таблица 6 – Лабораторные занятия и их трудоемкость

№ п/п	Наименование лабораторных работ	Трудоемкость, (час)	Из них практической подготовки, (час)	№ раздела дисциплины
Семестр 4				
1.	Законодательство в области ИБ. Сравнительный анализ Доктрин ИБ РФ.	2		2
2.	Анализ обрабатываемой информации с точки зрения видов тайн и требований к ее защите	4		3
3.	Исследование методов неформального оценивания и теории нечетких множеств	4		4
4.	Анализ методов и средств защиты информации с точки зрения угроз и их применения для объектов защиты	3		5, 6
5.	Анализ криптографических средств и систем защиты информации с точки зрения их развития	4		7
Всего		17		

4.5. Выполнение курсового проекта/ курсовой работы

Учебным планом не предусмотрено

4.6. Самостоятельная работа обучающихся

Виды самостоятельной работы и ее трудоемкость приведены в таблице 7.

Таблица 7 – Виды самостоятельной работы и ее трудоемкость

Вид самостоятельной работы	Всего, час	Семестр 4, час
1	2	3

Изучение теоретического материала дисциплины (ТО)	20	20
Курсовое проектирование (КП, КР)		
Расчетно-графические задания (РГЗ)		
Выполнение реферата (Р)		
Подготовка к текущему контролю успеваемости (ТКУ)	6	6
Домашнее задание (ДЗ)	12	12
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной аттестации (ПА)		
Всего:	38	38

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Учебно-методические материалы для самостоятельной работы обучающихся указаны в п.п. разделов 6-11.

6. Перечень печатных и электронных учебных изданий

Перечень печатных и электронных учебных изданий приведен в таблице 8.

Таблица 8– Перечень печатных и электронных учебных изданий

Шифр/ URL адрес	Библиографическая ссылка	Количество экземпляров в библиотеке (кроме электронных экземпляров)
УДК 004.056 ББК 32.973.202 Р95	Рындюк, В.А. методы и средства защиты информации: учеб.-метод. пособие/В.А. Рындюк. – СПб.: ГУАП, 2021. – 86с.	
УДК 004.056 Б 27	Басаргин А.А. Информационная безопасность и защита информации: практикум Сибирский государственный университет геосистем и технологий. Учебное пособие 2024. – 80 с.	
ISBN 978-5-507-55131-6	Баланов А.Н. Кибербезопасность: Учебное пособие для вузов. Издательство "Лань". 3-е изд., стер. 2026. — 680 с.	

7. Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины приведен в таблице 9.

Таблица 9 – Перечень электронных образовательных ресурсов информационно-телекоммуникационной сети «Интернет»

URL адрес	Наименование

http://www.intuit.ru/studies/courses/10/10/info	Владимир Галатенко. Основы информационной безопасности (курс лекций, с дистанционным обучением)

8. Перечень информационных технологий

8.1. Перечень программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине.

Перечень используемого программного обеспечения представлен в таблице 10.

Таблица 10– Перечень программного обеспечения

№ п/п	Наименование
	Не предусмотрено

8.2. Перечень информационно-справочных систем,используемых при осуществлении образовательного процесса по дисциплине

Перечень используемых информационно-справочных систем представлен в таблице 11.

Таблица 11– Перечень информационно-справочных систем

№ п/п	Наименование
	Не предусмотрено

9. Материально-техническая база

Состав материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине, представлен в таблице12.

Таблица 12 – Состав материально-технической базы

№ п/п	Наименование составной части материально-технической базы	Номер аудитории (при необходимости)
1	Лекционная аудитория	
2	Мультимедийная лекционная аудитория	
3	Компьютерный класс	

10. Оценочные средства для проведения промежуточной аттестации

10.1. Состав оценочных средствдля проведения промежуточной аттестации обучающихся по дисциплине приведен в таблице 13.

Таблица 13 – Состав оценочных средств для проведения промежуточной аттестации

Вид промежуточной аттестации	Перечень оценочных средств
Зачет	Список вопросов

10.2. В качестве критериев оценки уровня сформированности (освоения) компетенций обучающимися применяется 5-балльная шкала оценки сформированности компетенций, которая приведена в таблице 14. В течение семестра может использоваться 100-балльная шкала модульно-рейтинговой системы Университета, правила использования которой, установлены соответствующим локальным нормативным актом ГУАП.

Таблица 14 –Критерии оценки уровня сформированности компетенций

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
«отлично» «зачтено»	Обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«хорошо» «зачтено»	Обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«удовлетворительно» «зачтено»	– обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«неудовлетворительно» «не зачтено»	– обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

10.3. Типовые контрольные задания или иные материалы.

Вопросы (задачи) для экзамена представлены в таблице 15.

Таблица 15 – Вопросы (задачи) для экзамена

№ п/п	Перечень вопросов (задач) для экзамена	Код индикатора
	Учебным планом не предусмотрено	

Вопросы (задачи) для зачета представлены в таблице 16.

Таблица 16 – Вопросы для зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
1.	Предмет и задачи курса. Сущность информационной безопасности. Объекты информационной безопасности Связь информационной безопасности с информатизацией общества Значение информационной безопасности для субъектов информационных систем	ОПК-1.3.1

2.	Понятие и современная концепция национальной безопасности РФ. Место информационной безопасности в системе национальной безопасности РФ. Политика ИБ. Законодательство в области информационной безопасности. Современные стандарты ИБ.	ОПК-1.З.2
3.	Современные подходы к понятию угрозы защищаемой информации. Связь угрозы защищаемой информации с уязвимостью информации. Классификация угроз. Признаки и составляющие угрозы: явления, факторы, условия. Понятие угрозы защищаемой информации.	ОПК-1.З.3
4.	Деление угроз по видам, природе происхождения, по предпосылкам появления, по источникам. Структура факторов, создающих возможность дестабилизирующего воздействия на информацию.	ОПК-1.У.1
5.	Понятие объекта защиты. Виды и способы дестабилизирующего воздействия на объекты защиты. Классификация средств ЗИ. Основные средства ЗИ: программные, технические, организационные средства. Криптографические средства защиты. Стеганография.	ОПК-1.В.1
6.	Законодательство в области ИБ. Современные стандарты ИБ.	ОПК-5.В.1
7.	Политика ИБ. Законодательство в области информационной безопасности.	ОПК-8.З.1
8.	Принципы формирования политики информационной безопасности в информационных системах. Понятие систем защиты информации. Принципы построения СЗИ. Требования к СЗИ. Основы архитектурного построения СЗИ. Функциональное и организационное построение СЗИ. Понятия типизации и стандартизации СЗИ, их значение. Проектирование СЗИ.	ОПК-12.З.1

Перечень тем для выполнения курсового проекта/ курсовой работы представлены в таблице 17.

Таблица 17 – Перечень тем для выполнения курсового проекта / курсовой работы

№ п/п	Примерный перечень тем для выполнения курсового проекта/ курсовой работы
	Учебным планом не предусмотрено

Вопросы для проведения промежуточной аттестации в виде тестирования представлены в таблице 18.

Таблица 18 – Примерный перечень вопросов для тестов

№ п/п	Примерный перечень вопросов для тестов	Код индикатора
	Не предусмотрено	

Перечень тем контрольных работ по дисциплине обучающихся заочной формы обучения, представлены в таблице 19.

Таблица 19 – Перечень контрольных работ

№ п/п	Перечень контрольных работ
	Не предусмотрено

10.4. Методические материалы, определяющие процедуры оценивания индикаторов, характеризующих этапы формирования компетенций, содержатся в локальных нормативных актах ГУАП, регламентирующих порядок и процедуру проведения текущего контроля успеваемости и промежуточной аттестации обучающихся ГУАП.

11. Методические указания для обучающихся по освоению дисциплины

11.1. Методические указания для обучающихся по освоению лекционного материала

Основное назначение лекционного материала – логически стройное, системное, глубокое и ясное изложение учебного материала. Назначение современной лекции в рамках дисциплины не в том, чтобы получить всю информацию по теме, а в освоении фундаментальных проблем дисциплины, методов научного познания, новейших достижений научной мысли. В учебном процессе лекция выполняет методологическую, организационную и информационную функции. Лекция раскрывает понятийный аппарат конкретной области знания, её проблемы, дает цельное представление о дисциплине, показывает взаимосвязь с другими дисциплинами.

Планируемые результаты при освоении обучающимися лекционного материала:

– получение современных, целостных, взаимосвязанных знаний, уровень которых определяется целевой установкой к каждой конкретной теме;

– получение опыта творческой работы совместно с преподавателем;

– развитие профессионально-деловых качеств, любви к предмету и самостоятельного творческого мышления.

– появление необходимого интереса, необходимого для самостоятельной работы;

– получение знаний о современном уровне развития науки и техники и о прогнозе их развития на ближайшие годы;

– научиться методически обрабатывать материал (выделять главные мысли и положения, приходить к конкретным выводам, повторять их в различных формулировках);

– получение точного понимания всех необходимых терминов и понятий.

Лекционный материал может сопровождаться демонстрацией слайдов и использованием раздаточного материала при проведении коротких дискуссий об особенностях применения отдельных тематик по дисциплине.

Структура предоставления лекционного материала:

- Изложение лекционного материала;
- Представление теоретического материала преподавателем в виде слайдов;
- Освоение теоретического материала по практическим вопросам;
- Список заданий и вопросов по каждой теме для самостоятельной работы студента представлен в учебно- методическом пособии Рындюк В.А. «Методы и средства защиты информации».

11.2. Методические указания для обучающихся по выполнению лабораторных работ

В ходе выполнения лабораторных работ обучающийся должен углубить и закрепить знания, практические навыки, овладеть современной методикой и техникой эксперимента в соответствии с квалификационной характеристикой обучающегося. Выполнение лабораторных работ состоит из экспериментально-практической, расчетно-аналитической частей и контрольных мероприятий.

Выполнение лабораторных работ обучающимся является неотъемлемой частью изучения дисциплины, определяемой учебным планом, и относится к средствам, обеспечивающим решение следующих основных задач обучающегося:

– приобретение навыков исследования процессов, явлений и объектов, изучаемых в рамках данной дисциплины;

– закрепление, развитие и детализация теоретических знаний, полученных на лекциях;

– получение новой информации по изучаемой дисциплине;

– приобретение навыков самостоятельной работы с лабораторным оборудованием и приборами.

Задание и требования к проведению лабораторных работ

– В задании должно быть четко сформулирована задача, выполняемая в ЛР;

– Описаны входные и выходные данные для проведения ЛР;

– ЛР должна выполняться на основе полученных теоретических знаниях;

– Выполнение ЛР должно осуществляться на основе методических указаний, предоставляемых преподавателем;

– ЛР должна выполняться в специализированном компьютерном классе и может быть доработана студентом в домашних условиях, если позволяет ПО;

– Итогом выполненной ЛР является отчет.

Структура и форма отчета о лабораторной работе

– Постановка задачи;

– Входные и выходные данные;

– Содержание этапов выполнения;

– Обоснование полученного результата (вывод);

– Список используемой литературы.

Требования к оформлению отчета о лабораторной работе

– Лабораторная работа (ЛР) предоставляется в печатном/или электронном виде;

– ЛР должна соответствовать структуре и форме отчета, представленной выше;

– ЛР должна иметь титульный лист (ГОСТ 7.32-2001 издания 2008 года) с названием и подписью студента(ов), который(ые) ее сделал(и) и оформил(и);

– Студент должен защитить ЛР устно. Отметка о защите должна находиться на титульном листе вместе с подписью преподавателя.

11.3. Методические указания для обучающихся по прохождению самостоятельной работы

В ходе выполнения самостоятельной работы, обучающийся выполняет работу по заданию и при методическом руководстве преподавателя, но без его непосредственного участия.

В процессе выполнения самостоятельной работы у обучающегося формируется целесообразное планирование рабочего времени, которое позволяет ему развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивает высокий уровень успеваемости в период обучения, помогает получить навыки повышения профессионального уровня.

Методическими материалами, направляющими самостоятельную работу обучающихсяявляются:

– учебно-методический материал по дисциплине.

Примерный перечень тем для самостоятельного изучения:

– Системы управления доступом в Интернет и контроля корпоративной электронной почты.

– Утечки информации: источники, правовые и технологические аспекты.

– Утилизация данных: проблемы повторного использования.

– Методы защиты от нелегального использования ПО (и др. IT- ресурсов).
– Аспекты защиты информации в системах автоматизированного управления технологическими процессами.
– Особенности создания политики безопасности.
– Эволюция вредоносного ПО (malware) и средств борьбы с ним.
– Проблемы противодействия фишингу.
– P2P-приложения: тенденции развития и аспекты безопасности.
– Безопасность Web-браузеров.
– Безопасность беспроводных технологий.
– Виртуальные частные сети (VPN) – технологии и средства организации.
– Спам: способы распространения, принципы и средства. Противодействия
– Защита персональных данных, типовые решения.
– Биометрические системы аутентификации: принципы, технологии и перспективы.
– Средства взлома парольных систем и противодействие им.

11.4. Методические указания для обучающихся по прохождению текущего контроля успеваемости.

Текущий контроль успеваемости предусматривает контроль качества знаний обучающихся, осуществляемого в течение семестра с целью оценивания хода освоения дисциплины.

Форма проведения текущего контроля – защита отчетов по лабораторным работам и письменные ответы на вопросы по выбранной преподавателем теме. Результаты текущего контроля учитываются при проведении промежуточной аттестации в соответствии с требованиями СТО ГУАП. СМК 3.76 «Положение о текущем контроле успеваемости и промежуточной аттестации студентов и аспирантов ГУАП, обучающихся по образовательным программам высшего образования».

11.5. Методические указания для обучающихся по прохождению промежуточной аттестации.

Промежуточная аттестация обучающихся предусматривает оценивание промежуточных и окончательных результатов обучения по дисциплине. Она включает в себя:

– зачет – это форма оценки знаний, полученных обучающимся в ходе изучения учебной дисциплины в целом или промежуточная (по окончании семестра) оценка знаний обучающимся по отдельным разделам дисциплины с аттестационной оценкой «зачтено» или «не зачтено».

Проведение промежуточной аттестации подразумевает ответы студентов на вопросы к зачету.

Банк контрольных вопросов для промежуточной аттестации

Раздел 1. Введение. Сущность и понятие информационной безопасности.

1. Понятие безопасности информации. Цели и задачи защиты информации.
2. Основные проблемы защиты информации.
3. Этапы развития концепции обеспечения безопасности информации.
4. Необходимость развития теории безопасности, общие теоретические, методические принципы.

Раздел 2. Значение информационной безопасности и ее место в системе национальной безопасности

1. Государственная политика в информационной сфере.
2. Современная Доктрина информационной безопасности Российской Федерации.
3. Региональные проблемы информационной безопасности.
4. Современная концепция информационной безопасности.

Раздел 3. Состав и классификация защищаемой информации

1. Критерии, условия и принципы отнесения информации к защищаемой.
2. Оценки ценности информации. Количественная и качественная оценки.
3. Категории важности информации.
4. Классификация конфиденциальной информации по видам тайны и степеням конфиденциальности.
5. Государственная тайна, ее защита.
6. Коммерческая тайна, коммерческая информация, персональная информация, информация для внутреннего пользования.
7. Служебная тайна. Виды тайн.

Раздел 4. Теория защиты информации (ТЗИ). Методологический базис ТЗИ.

1. Теория защиты информации, общеметодологические принципы формирования теории защиты информации.
2. Модели систем и процессов защиты информации.
3. Особенности и состав научно-методологического базиса решения задач защиты информации.
4. Значение теории нечетких множеств для развития теории и практики ЗИ.
5. Нестрогая математика.
6. Неформальный поиск оптимальных решений.

Раздел 5. Понятие и структура угроз защищаемой информации.

1. Виды и типы угроз безопасности.
2. Классификация угроз.
3. Изменение активности угроз в зависимости от стадии жизненного цикла.
4. Формирование и коррекция кортесов потенциальных угроз.
5. Источники, виды и методы дестабилизирующего воздействия на защищаемую информацию.
6. Причины, обстоятельства и условия, вызывающие дестабилизирующее воздействие на защищаемую информацию.
7. Виды уязвимости информации и формы ее проявления.
8. Модель угроз.

Раздел 6. Классификация методов и средств защиты информации

1. Понятие методов защиты информации. Их классификация.
2. Методы препятствие, управление доступом, маскировка, регламентация, принуждение и побуждение.
3. Объекты защиты. Виды и способы дестабилизирующего воздействия на объекты защиты.
4. Средства защиты, их связь с методами защиты.
5. Классификация средств ЗИ.
6. Основные средства ЗИ: программные, технические, организационные средства.
7. Криптографические средства защиты, понятие и виды.
8. Симметричные, асимметричные и гибридные криптосистемы.
9. Стеганография.

Раздел 11. Системы защиты информации.

1. Понятие и принципы построения систем защиты информации.
2. Основы архитектурного построения систем защиты.
3. Функциональное, организационное и структурное построение систем защиты информации.
4. Типизация систем защиты. Классификация СЗИ при типизации
5. Стандартизация систем защиты.
6. Классификация СЗИ по активности реагирования и уровню защиты.
7. Уровни типизации и стандартизации.
8. Проектирование СЗИ.

Система оценок при проведении промежуточной аттестации осуществляется в соответствии с требованиями Положений «О текущем контроле успеваемости и промежуточной аттестации студентов ГУАП, обучающихся по программы высшего образования» и «О модульно-рейтинговой системе оценки качества учебной работы студентов в ГУАП».

Критерии оценки ответов на вопросы к зачету представлены в таблице 19.

Таблица 19 – Критерии оценки ответов на вопросы к зачету

Оценка ответа 5-балльная шкала	Характеристика ответа
«зачтено» («отлично»)	Ответ показал, что обучающийся: – глубоко и всесторонне усвоил программный материал; – уверенно, логично, последовательно и грамотно его излагает; – опираясь на знания основной и дополнительной литературы, тесно связывает усвоенные научные положения с практической деятельностью направления; – умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий.
«зачтено» («хорошо»)	Ответ показал, что обучающийся: – твердо усвоил программный материал, грамотно и по существу излагает его, опираясь на знания основной литературы; – не допускает существенных неточностей; – увязывает усвоенные знания с практической деятельностью направления; – аргументирует научные положения; – делает выводы и обобщения; – владеет системой специализированных понятий.
«зачтено» («удовлетворительно»)	Ответ показал, что обучающийся: – обучающийся усвоил только основной программный материал, по существу излагает его, опираясь на знания только основной литературы; – допускает несущественные ошибки и неточности; – испытывает затруднения в практическом применении знаний направления; – слабо аргументирует научные положения; – затрудняется в формулировании выводов и обобщений; – частично владеет системой специализированных понятий.
«не зачтено» («неудовлетворительно»)	Ответ показал, что обучающийся: – обучающийся не усвоил значительной части программного материала; – допускает существенные ошибки и неточности при

Оценка ответа 5-балльная шкала	Характеристика ответа
	рассмотрении проблем в конкретном направлении; – испытывает трудности в практическом применении знаний; – не может аргументировать научные положения; – не формулирует выводов и обобщений.

Лист внесения изменений в рабочую программу дисциплины

Дата внесения изменений и дополнений. Подпись внесшего изменения	Содержание изменений и дополнений	Дата и № протокола заседания кафедры	Подпись зав. кафедрой