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

зав.кафедрой, д.т.н.,проф.
(должность, уч. степень, звание)

С.В. Беззатеев
(инициалы, фамилия)

(подпись)

«20» февраля 2026 г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Техническая защита информации»
(Наименование дисциплины)

Код направления подготовки/ специальности	10.05.03
Наименование направления подготовки/ специальности	Информационная безопасность автоматизированных систем
Наименование направленности/ специализации	Безопасность открытых информационных 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.С. Коломойцев
(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 «Инженерно-технические средства защиты информации» входит в образовательную программу высшего образования – программу бакалавриата по направлению подготовки/ специальности 10.05.03 «Информационная безопасность автоматизированных систем» направленности/специализации «Безопасность открытых информационных систем». Дисциплина реализуется кафедрой «№33».

Дисциплина нацелена на формирование у выпускника следующих компетенций:

ПК-2 «Способен формировать требования к защите информации в открытых информационных системах»

ПК-7 «Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа»

ПК-10 «Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации»

Содержание дисциплины охватывает круг вопросов, связанных с анализом возможных угроз информационной безопасности объектов информатизации, преимущественно связанных с возможными утечками информации.

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

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена (7 семестр).

Общая трудоемкость освоения дисциплины составляет 3 зачетных единицы, 108 часов.

Язык обучения по дисциплине «русский»

1. Перечень планируемых результатов обучения по дисциплине

1.1. Цели преподавания дисциплины

Цели преподавания дисциплины состоят в получении знаний и умений по выбору средств технической защиты информации, пригодных для выполнения заданных функций в комплексной системе защиты информации объекта, комплексированию, определению оптимальных режимов работы и организации их эксплуатации в подсистеме инженерно технической защиты информации.

1.2. Дисциплина входит в состав части, формируемой участниками образовательных отношений, 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
Профессиональные компетенции	ПК-2 Способен формировать требования к защите информации в открытых информационных системах	ПК-2.З.2 знать программно-аппаратные средства обеспечения защиты информации автоматизированных систем ПК-2.У.5 уметь выявлять известные уязвимости информационных систем
Профессиональные компетенции	ПК-7 Способен управлять развитием средств защиты открытых информационных систем от несанкционированного доступа	ПК-7.З.1 знать порядок сертификации средств и систем защиты от несанкционированного доступа
Профессиональные компетенции	ПК-10 Способен осуществлять организацию работ по выполнению в автоматизированных системах требований защиты информации	ПК-10.У.1 уметь определять методы управления доступом, типы доступа и правила разграничения доступа ПК-10.В.1 владеть навыками формирования комплекса средств и мер для защиты информации в автоматизированных системах

2. Место дисциплины в структуре ОП

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

- «Основы информационной безопасности»,
- «Информатика»,
- «Основы информационной безопасности и методов защиты»,

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

- «Защита информации в распределенных информационных системах»,
- «ГИА»,
- «Проектирование безопасных информационных систем».

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
		№7
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	4/ 144	4/ 144
Из них часов практической подготовки	34	34
Аудиторные занятия, всего час.	68	68
в том числе:		
лекции (Л), (час)	34	34
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	34	34
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	36	36
Самостоятельная работа, всего (час)	40	40
***Вид промежуточной аттестации*:** зачет, дифф. зачет, экзамен (Зачет, Дифф. зач, Экз.)	Экз.,	Экз.,

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 7					
Введение Раздел 1. Обобщенная структура канала передачи информации	4				4
Раздел 2. Средства обработки информации. Защита от утечек и потерь информации.	6		15		12
Раздел 3. Оптический канал.	4		3		4
Раздел 4. Звуковой канал.	4		4		4
Текущий контроль	2				
Раздел 5. Каналы проводной связи.	4		4		5
Раздел 6. Каналы беспроводной связи	4		4		5
Раздел 7. Порядок и средства проведения контроля защищенности. Заключение	6		4		6
Итого в семестре:	34		34		40
Итого	34	0	34	0	40

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	**Введение. Раздел 1. Обобщенная структура канала передачи информации.** Требования к системе защиты информации. Содержание учебной дисциплины, порядок изучения. Основная и дополнительная литература. Каналы утечки информации. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Меры, препятствующие утечке информации.
2	**Раздел 2. Средства обработки информации. Защита от утечек и потерь информации.** Особенности использования компьютера как средства подготовки, передачи, получения и хранения информации. Съем информации с компьютера. Режимы работы компьютера.
3	**Раздел 3. Оптический канал.** Информация, распространяющаяся по оптическому каналу. Характерные особенности канала. Оптические приборы, используемые для получения информации, их характеристики. Преобразования оптического сигнала. Фиксация оптической информации. Защита от утечек информации.
4	**Раздел 4. Звуковой канал.** Защита от утечек информации. Характеристики информации, передаваемой по звуковому каналу. Приборы и преобразователи, используемые для получения и накопления информации, их характеристики и особенности функционирования. Способы защиты от утечек информации
5	**Раздел 5. Каналы проводной связи.** Устройство, функционирование и съем информации с телефона. Понятие о длинных линиях. Подключение к линиям проводной связи, способы его обнаружения. Защита от утечек информации
6	**Раздел 6 Каналы беспроводной связи.** Защита от утечек информации. Диапазоны радиоволн, особенности их распространения. Функции ГКРЧ. Структура, функционирование разведприемника. BYOD (Bring Your Own Devices) и средства защиты от них
7	**Раздел 7. Порядок и средства проведения контроля защищенности. Заключение.** Аудит инфраструктуры предприятия. Оценка защищенности предприятия от утечек

	по техническим каналам

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 7				
1	Устройство и безопасная эксплуатация компьютера	6	6	2
2	Live DVD системного администратора	6	6	2
3	Резервное копирование информации	6	6	2
4	Построение защищенной инфраструктуры предприятия от утечки информации по оптическому каналу	3	3	3
5	Построение защищенной инфраструктуры предприятия от утечки информации по звуковому каналу	4	4	4
6	Построение защищенной инфраструктуры предприятия от утечки информации по каналу проводной связи	4	4	5
7	Построение защищенной инфраструктуры предприятия от утечки информации по каналу беспроводной связи	4	4	6
8	Аудит инженерно-технической инфраструктуры защищенности предприятия	4	4	7
Всего		34	34	

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 7, час
1	2	3
Изучение теоретического материала дисциплины (ТО)	20	20
Подготовка к текущему контролю успеваемости (ТКУ)	5	5
Подготовка к промежуточной аттестации (ПА)	15	15
Всего:	40	40

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)
004 М 87	Защищенные инфотелекоммуникации. Анализ и синтез [Текст] : монография / Н. Н. Мошак ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - СПб. : Изд-во ГУАП, 2014. - 197 с.	40
004 М 87	Организация безопасного доступа к информационным ресурсам [Текст] : учебное пособие / Н. Н. Мошак, Т. М. Татарникова ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. -СПб. : Изд-во ГУАП, 2014. -	40

	121 с.	
http://e.lanbook.com/view/book/1122/	Шаньгин В.Ф. Защита компьютерной информации. ДМК Пресс, 2010. - 544 стр.	
http://znanium.com/bookread2.php?book=453862	Аверченков, В. И. Организационная защита информации [электронный ресурс] : учеб. пособие для вузов / В. И. Аверченков, М. Ю. Рытов. – 3-е изд., стереотип. – М. : ФЛИНТА, 2011. – 184 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
https://pro.guap.ru/	Материалы для выполнения практических работ, индивидуальные варианты для их выполнения, а также электронный лекционный материал по дисциплине размещаются внутри ЭИОС ГУАП «Интегрированная среда обучения» в течение учебного семестра

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
1	Электронная информационно-образовательная среда ГУАП «Интегрированная среда обучения» (https://pro.guap.ru/) разработана сотрудниками ГУАП (введена в эксплуатацию приказом ГУАП от 06.06.2017 № 05-215/17), перечень модулей и их функциональное назначение изложены по ссылке https://guap.ru/it/system/iso
2	Официальный сайт образовательной организации в сети «Интернет» (https://guap.ru/), разработан сотрудниками ГУАП (введен в эксплуатацию Приказом ГУАП от 23.03.2023 № 05-145/23)
3	LibreOffice 5 (Лицензия LGPLv3)

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
1	ЭБС Znanium (https://znanium.ru/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
2	ЭБС «Лань» (https://e.lanbook.com/), доступ через личный кабинет читателя библиотеки ГУАП, а также по IP -адресам ГУАП
3	Электронный каталог библиотеки ГУАП с доступом к базе полнотекстовых изданий (https://lib.guap.ru), доступ через личный кабинет читателя библиотеки ГУАП

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	Лаборатория технической защиты информации	14-34 (ул. Большая Морская, д.67, лит. А)

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
Экзамен	Список вопросов к экзамену; Экзаменационные билеты; Задачи; Тесты.

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;

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– умело обосновывает и аргументирует выдвигаемые им идеи; – делает выводы и обобщения; – свободно владеет системой специализированных понятий. – правильно выполнил от 90% до 100% тестовых заданий**.
«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. – правильно выполнил от 70% до 89% тестовых заданий**.
«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. – правильно выполнил от 51% до 69% тестовых заданий**.
«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. – правильно выполнил менее 51% тестовых заданий**.

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
1	Требования к системе защиты информации. Каналы утечки информации. ГОСТ Р 51275-2006 Защита информации.	ПК-7.З.1
2	Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Меры, препятствующие утечке информации. Особенности использования компьютера как средства подготовки, передачи, получения и хранения информации.	ПК-10.У.1
3	Съем информации с компьютера. Режимы работы компьютера. Защита от утечек информации в оптическом канале. Способы защиты от утечек информации в звуковом канале.	ПК-2.З.2

4	Защита от утечек информации в каналах проводной связи. Защита от утечек информации в каналах беспроводной связи.	ПК-10.В.1
5	Структура, функционирование разведприемника. BYOD (Bring Your Own Devices) и средства защиты от них. Порядок и средства проведения контроля защищенности.	ПК-2.У.5

Вопросы (задачи) для зачета / дифф. зачета представлены в таблице 16.

Таблица 16 – Вопросы (задачи) для зачета / дифф. зачета

№ п/п	Перечень вопросов (задач) для зачета / дифф. зачета	Код индикатора
	Учебным планом не предусмотрено	

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
	1. Кто является основным ответственным за определение уровня классификации информации? А. Руководитель среднего звена Б. Высшее руководство В. Владелец Г. Пользователь 2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? А. Сотрудники Б. Хакеры В. Атакующие Г. Контрагенты (лица, работающие по договору) 3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? А. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования Б. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации В. Улучшить контроль за безопасностью этой информации Г. Снизить уровень классификации этой информации	ПК-7.З.1

	4. Что самое главное должно продумать руководство при классификации данных? А. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным Б. Необходимый уровень доступности, целостности и конфиденциальности В. Оценить уровень риска и отменить контрмеры Г. Управление доступом, которое должно защищать данные 5. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? А. Владельцы данных Б. Пользователи В. Администраторы Г. Руководство 6. Что такое процедура? А. Правила использования программного и аппаратного обеспечения в компании Б. Пошаговая инструкция по выполнению задачи В. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах Г. Обязательные действия.	
	7. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? А. Поддержка высшего руководства Б. Эффективные защитные меры и методы их внедрения В. Актуальные и адекватные политики и процедуры безопасности Г. Проведение тренингов по безопасности для всех сотрудников 8. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков? А. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски Б. Когда риски не могут быть приняты во внимание по политическим соображениям В. Когда необходимые защитные меры слишком сложны Г. Когда стоимость контрмер превышает ценность актива и потенциальные потери 9. Что такое политики безопасности? А. Пошаговые инструкции по выполнению задач безопасности Б. Общие руководящие требования по достижению определенного уровня безопасности В. Широкие, высокоуровневые заявления руководства Г. Детализированные документы по обработке инцидентов безопасности	ПК-10.У.1
	10. Какая из приведенных техник является самой важной при выборе конкретных защитных мер? А. Анализ рисков Б. Анализ затрат / выгоды В. Результаты ALE	ПК-2.З.2

	Г. Выявление уязвимостей и угроз, являющихся причиной риска 11. Что лучше всего описывает цель расчета ALE? А. Количественно оценить уровень безопасности среды Б. Оценить возможные потери для каждой контрмеры В. Количественно оценить затраты / выгоды Г. Оценить потенциальные потери от угрозы в год 12. Тактическое планирование – это: А. Среднесрочное планирование Б. Долгосрочное планирование В. Ежедневное планирование Г. Планирование на 6 месяцев 13. Что является определением воздействия (exposure) на безопасность? А. Нечто, приводящее к ущербу от угрозы Б. Любая потенциальная опасность для информации или систем В. Любой недостаток или отсутствие информационной безопасности Г. Потенциальные потери от угрозы	
	14. Эффективная программа безопасности требует сбалансированного применения: А. Технических и нетехнических методов Б. Контрмер и защитных механизмов В. Физической безопасности и технических средств защиты Г. Процедур безопасности и шифрования 15. Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют: А. Внедрение управления механизмами безопасности Б. Классификацию данных после внедрения механизмов безопасности В. Уровень доверия, обеспечиваемый механизмом безопасности Г. Соотношение затрат / выгод 16. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации? А. Только военные имеют настоящую безопасность Б. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности В. Военным требуется больший уровень безопасности, т.к. их риски существенно выше Г. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности.	ПК-10.В.1
	17. Как рассчитать остаточный риск? А. Угрозы х Риски х Ценность актива Б. (Угрозы х Ценность актива х Уязвимости) х Риски В. SLE х Частоту = ALE Г. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля	ПК-2.У.5

	18. Что из перечисленного не является целью проведения анализа рисков? А. Делегирование полномочий Б. Количественная оценка воздействия потенциальных угроз В. Выявление рисков Г. Определение баланса между воздействием риска и стоимостью необходимых контрмер 19. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности? А. Поддержка Б. Выполнение анализа рисков В. Определение цели и границ Г. Делегирование полномочий 20. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании? А. Чтобы убедиться, что проводится справедливая оценка Б. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ В. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа Г. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку 21. Что является наилучшим описанием количественного анализа рисков? А. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности Б. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков В. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков Г. Метод, основанный на суждениях и интуиции 22. Почему количественный анализ рисков в чистом виде не достижим? А. Он достижим и используется Б. Он присваивает уровни критичности. Их сложно перевести в денежный вид. В. Это связано с точностью количественных элементов Г. Количественные измерения должны применяться к качественным элементам 23. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?	

	А. Много информации нужно собрать и ввести в программу Б. Руководство должно одобрить создание группы В. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки Г. Множество людей должно одобрить данные 24. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств? А. Стандарты Б. Должный процесс (Due process) В. Должная забота (Due care) Г. Снижение обязательств 25. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности? А. Список стандартов, процедур и политик для разработки программы безопасности Б. Текущая версия ISO 17799 В. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях Г. Открытый стандарт, определяющий цели контроля.	

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:

Введение. Требования к системе защиты информации. Содержание учебной дисциплины, порядок изучения. Основная и дополнительная литература.

Раздел 1. Обобщенная структура канала передачи информации.

Раздел 2. Средства обработки информации. Защита от утечек и потерь информации.

Раздел 3. Оптический канал.

Раздел 4. Звуковой канал.

Раздел 5. Каналы проводной связи.

Раздел 6 Каналы беспроводной связи.

Раздел 7. Порядок и средства проведения контроля защищенности.

Заключение

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

Вариант выполнения лабораторного задания выдается на основе порядкового номера студента в списке учебной группы. Вариант лабораторной работы влияет на начальные (вводные) условия для выполнения задания. В рамках заданий лабораторной работы студенту требуется:

1. Используя существующие методики безопасной эксплуатации СВТ, разработать проект мер обеспечения защищенности компьютера при его работе в сети Интернет и внутри корпоративной сети.

2. Разработать план построения Live DVD системного администратора, с подбором программных средств, который может позволить обеспечить восстановление штатной работы операционной системы компьютера.
3. Выработать набор мер по резервному копированию информации (с учетом специфики рабочего места пользователя, на основе варианта задания), находящейся на СВТ.
4. При наличии сформированных инженерных ограничений предприятия, требуется построить инфраструктурный план инженерно-технической системы защиты предприятия от утечки информации по оптическому каналу. Требуется учесть возможности потенциального нарушителя, ограничения контролируемых зон, а также технические возможности по обеспечению защиты от утечки по указанному каналу.
5. При наличии сформированных инженерных ограничений предприятия, требуется построить инфраструктурный план инженерно-технической системы защиты предприятия от утечки информации по звуковому каналу. Требуется учесть возможности потенциального нарушителя, ограничения контролируемых зон, а также технические возможности по обеспечению защиты от утечки по указанному каналу.
6. При наличии сформированных инженерных ограничений предприятия, требуется построить инфраструктурный план инженерно-технической системы защиты предприятия от утечки информации по проводному каналу. Требуется учесть возможности потенциального нарушителя, ограничения контролируемых зон, а также технические возможности по обеспечению защиты от утечки по указанному каналу.
7. При наличии сформированных инженерных ограничений предприятия, требуется построить инфраструктурный план инженерно-технической системы защиты предприятия от утечки информации по беспроводному каналу. Требуется учесть возможности потенциального нарушителя, ограничения контролируемых зон, а также технические возможности по обеспечению защиты от утечки по указанному каналу.
8. Используя результаты построения инфраструктурных планов инженерно-технической системы защиты предприятия от утечки информации по различным каналам, обеспечить комплексную непротиворечивую (в нормативном, организационном и техническом плане) защиту предприятия от утечки информации по техническим каналам. Следует учитывать специфику работы предприятия (его бизнес-процессы), а также контролируемые зоны. Провести аудит, построенной системы, на предмет реализации возможных угроз информационной безопасности, нарушителем.

Структура и форма отчета о лабораторной работе

Отчет о лабораторной работе должен включать в себя: титульный лист, формулировку задания, теоретические положения, используемые при выполнении лабораторной работы, описание процесса выполнения лабораторной работы, полученные результаты и выводы.

Требования к оформлению отчета о лабораторной работе

По каждой лабораторной работе выполняется отдельный отчет. Титульный лист оформляется в соответствии с шаблоном (образцом) приведенным на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации». Текстовые и графические материалы оформляются в соответствии с действующими ГОСТами и требованиями,

приведенными на сайте ГУАП (www.guap.ru) в разделе «Сектор нормативной документации».

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.

Для обучающихся по заочной форме обучения выполнение контрольных работ является элементом текущего контроля успеваемости и самостоятельной работы

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;

– методические указания по выполнению контрольных работ (для обучающихся по заочной форме обучения).

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. 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:

– экзамен – форма оценки знаний, полученных обучающимся в процессе изучения всей дисциплины или ее части, навыков самостоятельной работы, способности применять их для решения практических задач. Экзамен, как правило, проводится в период экзаменационной сессии и завершается аттестационной оценкой «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

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».

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