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 управления информационной безопасностью»
(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)

проф.,д.т.н.,проф.	20.02.26	С.Г. Фомичева
(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 управления информационной безопасностью» 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-5 «Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности»

ОПК-6 «Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю»

ОПК-10 «Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты»

ОПК-1.4 «Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями»

Содержание дисциплины охватывает круг вопросов, связанных с изучением методов и средств управления информационной безопасностью (ИБ) в организации, а также изучением основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объекта.

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

Программой дисциплины предусмотрены следующие виды контроля: текущий контроль успеваемости, промежуточная аттестация в форме экзамена (8 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

- приобретение необходимого объема знаний и практических навыков по управлению информационной безопасностью, оценки рисков информационных ресурсов организации и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность;
– формирование представления о содержании процессов управления информационной безопасностью организации как результата внедрения системного подхода к решению задач обеспечения информационной безопасности

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

1.2. 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-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.З.4 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности ОПК-5.У.4 умеет формулировать основные требования по защите конфиденциальной информации, персональных данных и охране результатов интеллектуальной деятельности в организации
Общепрофессиональные компетенции	ОПК-6 Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности	ОПК-6.З.3 знает систему организационных мер, направленных на защиту информации ограниченного доступа ОПК-6.З.5 знает основные угрозы безопасности информации и модели нарушителя объекта информатизации ОПК-6.У.1 умеет разрабатывать модели угроз и модели нарушителя объекта информатизации ОПК-6.У.2 умеет разрабатывать проекты инструкций, регламентов, положений и приказов, регламентирующих защиту информации ограниченного доступа в организации ОПК-6.У.3 умеет определить политику контроля доступа работников к информации ограниченного доступа

	Российской Федерации, Федеральной службы по техническому и экспортному контролю	ОПК-6.У.4 умеет формулировать основные требования, предъявляемые к физической защите объекта и пропускному режиму в организации
Общепрофессиональные компетенции	ОПК-10 Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.З.2 знает правовые основы организации защиты персональных данных и охраны результатов интеллектуальной деятельности ОПК-10.З.3 знает принципы формирования политики информационной безопасности организации
Общепрофессиональные компетенции по направленности	ОПК-1.4 Способен оценивать уровень безопасности компьютерных систем и сетей, в том числе в соответствии с нормативными и корпоративными требованиями	ОПК-1.4.У.1 умеет определять уровень безопасности и соответствие профилю защиты ОПК-1.4.У.2 умеет анализировать угрозы безопасности информации в компьютерных системах и сетях

2. Место дисциплины в структуре ОП

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

- Технологии и методы программирования»
- «Основы информационной безопасности»
- «Безопасность сетей ЭВМ»
- «Теория информационной безопасности»

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

- « Производственная преддипломная практика»,
- «Государственная итоговая аттестация»

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
		№8
1	2	3
Общая трудоемкость дисциплины, ЗЕ/ (час)	3/ 108	3/ 108
Из них часов практической подготовки		
Аудиторные занятия, всего час.	40	40
в том числе:		
лекции (Л), (час)	20	20
практические/семинарские занятия (ПЗ), (час)		
лабораторные работы (ЛР), (час)	20	20
курсовой проект (работа) (КП, КР), (час)		
экзамен, (час)	27	27
Самостоятельная работа, всего (час)	41	41
***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 8					
Раздел 1. Общие вопросы организации управления информационной безопасностью	4		4		3
Раздел 2. Политика безопасности организации	4		4		8
Раздел 3. Системы управления ИБ	4		4		10
Раздел 4. Основы управления рисками ИБ	4		4		10
Раздел 5. Процессы управления ИБ	4		4		10
Итого в семестре:	20		20		41
Итого	20	0	20	0	41

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. Общие вопросы организации управления информационной безопасностью** Тема 1.1. Введение Понятие процесса управления ИБ Тема 1.2. Процессный подход регуляторов к «Обеспечению информационной безопасности» Тема 1.3. Базовые вопросы управления ИБ. Уровни управления информационной безопасностью Тема 1.4. Стандартизация в области управления ИБ
2	**Раздел 2. Моделирование УБИ и Политика безопасности организации** Тема 2.1. Методы выявления и анализа угроз безопасности Информации. Модель угроз безопасности информации (УБИ) Тема 2.2. Методы выявления и анализа уязвимостей. Общая система оценки уязвимостей CVSS Тема 2.3. Типы и виды Политик ИБ. Свойства эффективной Политики ИБ. Формирование политики информационной безопасности Тема 2.4. Модель защиты. Профили безопасности
3	**Раздел 3. Системы управления ИБ** Тема 3.1. Функции и состав системы управления информационной Принципы функционирования SIEM - Security Information and Event Management. Эволюция SIEM Тема 3.2. Архитектура SIEM : технология, процесс и данные. Тема 3.3 Модели хостинга SIEM Тема 3.4. Формирование SIEM-экосистемы. Организация тестового окружения Тема 3.5 Менеджмент событий безопасности
4	**Раздел 4. Основы управления рисками ИБ** Тема 4.1. Стандартизация в сфере аудита информационной безопасности. Тема 4.2. Содержание и организация процесса аудита информационной безопасности. Тема 4.3. Оценка рисков информационной безопасности. Метод оценки рисков на основе модели угроз и уязвимостей.
5	**Раздел 5. Процессы управления ИБ** Тема 5.1 Структура современного SOC и метрики его производительности Тема 5.2 Принципы аналитики поведения пользователя и сущностей (UEBA) Тема 5.3. Фиды. Индикаторы атак. Индикаторы компрометации. Приоритизация индикаторов компрометации Тема 5.4. Поведенческая оценка и оценка рисков Тема 5.4 Реагирование на инциденты безопасности

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 8				
1	Описание объекта исследования с точки зрения инженера (администратора) по информационной безопасности	4	4	1
2	Формирование частной модели угроз безопасности информации	4	4	2
3	Разработка политик безопасности информации	4	4	2
4	Формирование SIEM-экосистемы	4	4	3
5	Управление событиями безопасности	4	4	4,5
Всего		20	20	

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 8, 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)	10	10
Домашнее задание (ДЗ)		
Контрольные работы заочников (КРЗ)		
Подготовка к промежуточной	11	11

аттестации (ПА)		
Всего:	41	41

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 З-40	Защита информации : учебное пособие / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Москва : РИОР : ИНФРА-М, 2023. - 400 с. : рис. - (Высшее образование). - Библиогр.: с. 393 - 396 (55 назв.). - ISBN 978-5-369-01759-3 : 2323.88 р. - Текст : непосредственный. Имеет гриф УМО по образованию в области информационных технологий и систем связи	15
004 Б 39	**С. В. Беззатеев, С. Г. Фомичева.** SIEM-системы в управлении информационной безопасностью : учебное пособие / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2021. - 131 с. : рис., табл. - Библиогр.: с. 128- 130 (28 назв.). - ISBN 978-5-8088-1676-3	4
004 Ф 76	Разработка моделей угроз безопасности информации: Методические указания. Составитель: С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 89 с. : рис., табл.	5
004 Ф 76	**С. Г. Фомичева.** Защита распределенных информационных систем : учебно-методическое пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2022. - 55 с. : рис., табл. - Библиогр.: с. 54 (10 назв.).	5
004 Ф 76	**С. Г. Фомичева.** Методы машинного обучения в задачах обеспечения информационной безопасности : учебное пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 136 с. :	5

	рис. - Библиогр.: с. 131 - 133 (29 назв.). - ISBN 978-5-8088-1822-4	
004 И-98	**Ищейнов, В. Я.** Основные положения информационной безопасности : учебное пособие / В. Я. Ищейнов, М. В. Мецатунян. - Москва : ФОРУМ: ИНФРА-М, 2024. - 208 с. : рис. - (Среднее специальное образование). - Библиогр.: с. 204 - 205 (19 назв.). - ISBN 978-5-00091-489-2 : 1266.30 р.	10

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://infosecportal.ru/category/standarty/	Стандарты ИБ
https://infosecportal.ru/category/zakonodatelstvo/	Законы в сфере ИБ
https://bdu.fstec.ru/threat	Банк УБИ ФСТЭК
https://bdu.fstec.ru/vul	Банк Уязвимостей ФСТЭК
https://bduasutp.fstec.ru/#/	Банк данных угроз безопасности информации в автоматизированных системах управления технологическими процессами

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	https://bdu.fstec.ru/site/scanoval Программа ScanOVAL для автоматизированных проверок наличия уязвимостей программного обеспечения
2	https://wazuh.com/ - Wazuh Платформа безопасности с открытым исходным кодом
3	https://www.misp-project.org/ - MISP - Платформа для анализа и обмена информацией об угрозах с открытым исходным кодом
4	https://github.com/fisher85/AirSIEM - Учебный проект AirSIEM
5	Операционные системы MS Windows, Linux.
6	Среда разработки MS Visual Studio

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	

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.

Примечание: *экзаменационные билеты формируются на основе вопросов и задач таблицы 15.

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. – 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;

Оценка компетенции 5-балльная шкала	Характеристика сформированных компетенций
	– 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. Цели и задачи управления информационной безопасностью 2. Архитектура системы обеспечения информационной безопасности Роль политики безопасности в задачах управления информационной безопасностью. 3. Стандарты управления информационной безопасностью Международный стандарт ISO/IEC 27001:2005 «Системы управления информационной безопасности. Требования». 4. Сертификация систем управления информационной безопасностью на соответствие ISO 27001. 5. Структура и функции системы управления информационной безопасностью 6. Политика безопасности и ее роль в управлении информационной безопасностью 7. Этапы создания системы управления ИБ. Категорирование активов компании. 8. Оценка защищенности информационной системы компании. 9. Оценка информационных рисков. 10. Методика оценки рисков информационной безопасности компании. 11. Управление рисками. Основные понятия. 12. Метод оценки рисков на основе модели угроз и уязвимостей. 13. Метод оценки рисков на основе модели информационных потоков. 14. Качественные методики управления рисками. 15. Количественные методики управления рисками. Управление	ОПК-5.З.4 ОПК-5.У.4 ОПК-6.З.3 ОПК-6.З.5 ОПК-6.У.1 ОПК-6.У.2 ОПК-6.У.3 ОПК-6.У.4 ОПК-10.З.2 ОПК-10.З.3 ОПК-1.4.У.1 ОПК-1.4.У.2

	средствами защиты информации. 16. Правовые основы аудита информационной безопасности Место и роль аудита в управлении информационной безопасности 17. Методология проведения аудита информационной безопасности 18. Менеджмент аудита информационной безопасности 19. Методы оценки эффективности информационной безопасности 20. Способы анализ результатов аудита информационной безопасности 21. Нормативно-технические документы аудита информационной безопасности 22. Виды контроля состояния информационной безопасности объектов 23. Методы анализа состояния информационной безопасности	

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.	К какой разновидности моделей управления доступом относится модель Белла-Ла Падулы? а) модель дискреционного доступа; б) модель мандатного доступа; в) ролевая модель.	ОПК-6.У.1
2.	Как называются угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.?	ОПК-6.З.5
3.	К каким мерам защиты относится применение политик информационной безопасности? а) к административным; б) к законодательным; в) к программно-техническим; г) к процедурным.	ОПК-6.З.3
4.	В каком из представлений матрицы доступа наиболее просто определить пользователей, имеющих доступ к определенному файлу? а) ACL; б) списки полномочий субъектов; в) атрибутные схемы.	ОПК-5.У.4

5.	Как называется свойство информации, означающее отсутствие неправомочных, и не предусмотренных ее владельцем изменений? а) целостность; б) апеллируемость; в) доступность; г) конфиденциальность; д) аутентичность	ОПК-6.У.4
6.	К основным принципам построения системы управления информационной безопасностью относятся: а) открытость; б) взаимозаменяемость подсистем защиты; в) минимизация привилегий; г) комплексность; д) простота	ОПК-5.У.4
7.	Какие из следующих высказываний о модели управления доступом RBAC справедливы? а) с каждым субъектом (пользователем) может быть ассоциировано несколько ролей; б) роли упорядочены в иерархию; в) с каждым объектом доступа ассоциировано несколько ролей; г) для каждой пары «субъект-объект» назначен набор возможных разрешений	ОПК-6.У.2
8.	Диспетчер доступа... а) ... использует базу данных защиты, в которой хранятся правила разграничения доступа; б) ... использует атрибутные схемы для представления матрицы доступа; в) ... выступает посредником при всех обращениях субъектов к объектам; г) ... фиксирует информацию о попытках доступа в системном журнале;	ОПК-6.У.3
9.	Какие предположения включает неформальная модель нарушителя? а) о возможностях нарушителя; б) о категориях лиц, к которым может принадлежать нарушитель; в) о привычках нарушителя; г) о предыдущих атаках, осуществленных нарушителем; д) об уровне знаний нарушителя	ОПК-6.З.3 ОПК-6.У.1
10.	Что представляет собой доктрина информационной безопасности РФ? а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности; б) федеральный закон, регулирующий правоотношения в области информационной безопасности; в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов; г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации	ОПК-5.З.4
11.	Субъект управления — это	ОПК-

	а) лицо, группа людей или организация, принимающие решения и управляющие объектами, процессами или отношениями путём воздействия на управляемую систему для достижения поставленных целей; б) термин кибернетики и теории автоматического управления, обозначающий устройство или динамический процесс, управление поведением которого является целью создания системы автоматического управления; в) Наука, изучающая структуру, общие свойства и методы передачи информации, в том числе связанной с применением ЭВМ. г) Состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.	10.З.2
12.	Что такое политика безопасности? а) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности; б) Наука, изучающая структуру, общие свойства и методы передачи информации, в том числе связанной с применением ЭВМ; в) Совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации; г) Документы по обработке инцидентов безопасности.	ОПК-10.З.2
13.	Управление информационной безопасностью – это а) Циклический процесс, включающий осознание степени необходимости защиты информации и постановку задач; б) Тот, кто в силу своего служебного или семейного положения имеет доступ к конфиденциальной информации о делах компании; в) Наука, изучающая структуру, общие свойства и методы передачи информации, в том числе связанной с применением ЭВМ; г) Наиболее общая модель защиты автоматизированных систем, базирующаяся на том, что система безопасности должна иметь по крайней мере одно средство.	ОПК-6.У.2
14.	Событие информационной безопасности — это а) Единичное событие или ряд нежелательных и непредвиденных событий информационной безопасности, из-за которых велика вероятность компрометации информации и угрозы информационной безопасности.; b) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков; c) Идентифицированный случай состояния системы или сети, указывающий на возможное нарушение политики информационной безопасности или отказ средств защиты, либо ранее неизвестная ситуация, которая может быть существенной для безопасности; d) Метод, основанный на суждениях и интуиции.	ОПК-6.У.4
15.	Инцидентом информационной безопасности называют а) Нежелательное событие ИБ (или совокупность событий),	ОПК-10.З.3

	которое может скомпрометировать бизнес- процессы компании или непосредственно угрожает ее информационной безопасности и нарушает политику ИБ; b) Обобщающий термин кибернетики и теории автоматического управления, обозначающий устройство или динамический процесс, управление поведением которого является целью создания системы автоматического управления; c) Наука, изучающая структуру, общие свойства и методы передачи информации, в том числе связанной с применением ЭВМ; d) Состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере.	
16.	Кто не участвует в процессе реагирования на инцидент? a) Юристы; b) Технические эксперты ИТ-системы; c) Внешние консультанты по информационной безопасности; d) Простые рабочие.	ОПК-6.У.4
17.	Что в первую очередь необходимо предпринять при обнаружении инцидента А) Действия, останавливающие или замедляющие развитие событий Б) Расследование инцидента В) Восстановление затронутых ресурсов Г) Сообщение об инциденте по соответствующим каналам	ОПК-6.У.3
18.	Управление риском – это: а) отказ от рискованного проекта; б) комплекс мер, направленных на снижение вероятности реализации риска; в) комплекс мероприятий, направленных на подготовку к реализации риска.	ОПК-1.4.У.1
19.	Является ли мониторинг событий безопасности контрольной процедурой аудита? а) да б) нет	ОПК-1.4.У.2
20.	Справедливо ли, что утверждение политики информационной безопасности организации должен пройти через отдел кадров и юридический отдел а) да б) нет	ОПК-10.З.3
21.	Справедливо ли утверждение – управление информационной безопасностью построено на процессном подходе а) да б) нет	ОПК-10.З.3
22.	Делегирование – это: а). обязанность обеспечить позитивное решение поставленных задач б) Направление усилий подчиненных на выполнение задания. в) Передача заданий и полномочий лицу, что берет на себя ответственность за их выполнение.	ОПК-6.У.4
23.	Какой стандарт устанавливает требования к системам менеджмента информационной безопасности (СМИБ)	ОПК-5.З.4

	а) ИСО 17709 б) ИСО 27001 в) 152-ФЗ г) 235-ФЗ	

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 вопросов по теме для самостоятельной работы студента

Если методические указания по освоению лекционного материала имеются в изданном виде, в виде электронных ресурсов библиотеки ГУАП, системы LMS, кафедры и т.д., необходимо дать на них ссылку или привести URL адрес.

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

Лабораторная работа № 1. «Описание объекта исследования с точки зрения инженера (администратора) по информационной безопасности»

Цели лабораторной работы № 1: Построение различных моделей, отображающих архитектуру автоматизированной системы, ограничений доступа к информации и проведение анализа мест и видов утечки информации. Оценка степени защищенности информации

Лабораторная работа №1 состоит из двух частей – общей и индивидуальной.

Общая часть лабораторной работы (ЛР) выполняется всеми студентами и содержит те же этапы, что и индивидуальная часть.

Общая часть выполняется для рассмотренного в методических рекомендациях (см. ниже) конкретного объекта защиты – информационной системы «Cyber Marker», предназначенной для автоматического ранжирования индикаторов компрометации. В ходе реализации общей части ЛР1 дублируются действия, непосредственно отраженные в методических рекомендациях (без изменений). Успешное выполнение ТОЛЬКО общей части оценивается оценкой «**удовлетворительно**». Общая часть служит образцом для выполнения индивидуальной части.

Индивидуальная часть предусматривает самостоятельный выбор студентом объекта защиты и выполнения полного комплекса ниже следующих действий (Общая часть при этом также должна быть выполнена). Объектом защиты может служить любая ранее разработанная студентом информационная система (или, по меньшей мере, программный продукт с функционалом логирования исключений и/или событий безопасности). Перечень вариантов таких объектов защиты приведен в приложении 1 к методическим рекомендациям. Требования к оформлению отчетов по лабораторным работам приведены в методических указаниях С.Г. Фомичева «Моделирование угроз при управлении информационной безопасностью», размещенных в разделе «Материалы» личного кабинета АИС «ГУАП»

Задание к ЛР№1

В ходе выполнения лабораторной работы №1 (как общей, так и индивидуальной части) требуется:

1) Выполнить оценку необходимости защиты разрабатываемой и/или эксплуатируемой информационной системы (объекта защиты).

2) Установить и освоить навыки использования инструментария структурного (в соответствии с методологией IFEFX) и/или объектного (в соответствии с методологией UML) системного анализа.

3) Провести структурный и/или объектный системный анализ бизнес-процессов предметной области. Построить диаграммы IDEF0 (AS-IS), DFD (AS-IS), (при необходимости – IDEF3 (AS-IS). В случае объектного анализа построить соответствующие UML-диаграммы.

4) Описать разработанные диаграммы в соответствии с требованиями ISO 9000:9100.

5) Сформулировать выводы по лабораторной работе

Структура и форма отчета о лабораторной работе

Отчет по ЛР должен содержать цель и задачи ЛР; совокупность диаграмм IDEF0 (AS-IS), DFD (AS-IS) или соответствующие UML-диаграммы с контекстным их описанием; выводы по лабораторной работе,

Требования к оформлению отчета о лабораторной работе и методические рекомендации по выполнению ЛР приведены в методических указаниях «Разработка моделей угроз безопасности информации»: Методические указания. Составитель: С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 89 с.

Лабораторная работа №2 «Формирование частной модели угроз безопасности информации»

Лабораторная работа №2 является основным этапом построения систем защиты, в ходе которого, собственно, и производится формирование модели угроз безопасности информации (УБИ). Данная модель является основой построения модели защиты для проектируемой или эксплуатируемой информационной системы.

Цели лабораторной работы № 2: Построение инфологических моделей для защищенных ИС и баз данных с защищенными атрибутами и установленными правами, и привилегиями доступа к данным. Формирование частной модели угроз безопасности информации».

Задание к лабораторной работе № 2

В ходе выполнения лабораторной работы №2 требуется:

1) Провести структурный и/или объектный системный анализ бизнес-процессов предметной области. Построить диаграммы IDEF0 (TO-BE), DFD (TO-BE), (при необходимости – IDEF3 (TO-BE). В случае объектного анализа построить соответствующие UML-диаграммы.

2) Описать разработанные диаграммы в соответствии с требованиями ISO 9000:9100.

3) Выделить активы (критические элементы), подлежащие информационной защите

4) Определить вид обеспечения безопасности информации для каждого актива.

5) Построить модель нарушителя.

6) Сформировать реестр актуализированных угроз для каждого актива.

7) Построить частную модель угроз разрабатываемой информационной системы.

8) Сформулировать выводы по разделу

Структура и форма отчета о лабораторной работе

Отчет по ЛР должен содержать цель и задачи ЛР; совокупность диаграмм IDEF0 (To-Be) DFD (To-Be) или соответствующие UML-диаграммы с контекстным их описанием; таблицы с актуальными УБИ, активами и видами обеспечения их безопасности; схему с частной моделью УБИ; выводы по лабораторной работе,

Требования к оформлению отчета о лабораторной работе и методические рекомендации по выполнению ЛР приведены в методических указаниях «Разработка моделей угроз безопасности информации»: Методические указания. Составитель: С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 89 с.

Лабораторная работа №3 «Разработка политик безопасности информации»

Сформированная на этапе №2 модель угроз безопасности информацию позволяет перейти к формулированию целей безопасности, разработке правил политик безопасности для достижения данных целей. В свою очередь политика информационной безопасности является фундаментом модели защиты.

Цели лабораторной работы №3 - оценка защищенности информационной системы, формирование корпоративной и частных политик информационной безопасности, реализующих требуемый уровень защищенности системы.

Задание к Лабораторной работе №3

В ходе выполнения лабораторной работы №3 требуется:

1) На основании предположений безопасности, при учете угроз и имеющихся уязвимостей (модели угроз, полученной в ходе выполнения лабораторной работы № 2) сформулировать цели безопасности, определить класс и категорию защищенности информационной (автоматизированной) системы.

2) Руководствуясь ГОСТ Р ИСО/МЭК ТО 13335, ГОСТ и ГОСТ Р ИСО/МЭК 27001 выполнить априорную оценку и приоритизацию рисков, а также соблюдение законодательных и нормативных актов для рассматриваемой информационной системы

3) Результаты экспертной оценки рисков ИБ, полученные на предыдущем шаге использовать для формирования корпоративной и необходимого числа частных политик, позволяющих привести защищаемую систему к соответствию ISO 27001 с учетом приоритизации рисков.

4) Провести оценку защищенности, эксплуатируемой или проектируемой информационной системы с учетом адаптации правил политик информационной безопасности (красных кружков в экспертной оценке не должно остаться). Использовать инструмент оценки рисков Microsoft Security Assessment Tool (MSAT)– https://www.microsoft.com/ru-ru/download/details.aspx?id=12273 или иного программного средства оценки рисков ИБ

5) Выделить в политиках информационной безопасности внесенные изменения.

6) Определить эффективность внесения изменений в политику информационной безопасности.

7) Оформить отчет по лабораторной работе №3

Структура и форма отчета о лабораторной работе

Отчет по ЛР должен содержать цель и задачи ЛР; результаты оценки рисков ИБ и правила политик безопасности, снижающие риски ИБ; выводы по лабораторной работе,

Требования к оформлению отчета о лабораторной работе и методические рекомендации по выполнению ЛР приведены в методических указаниях «Разработка моделей угроз безопасности информации»: Методические указания. Составитель: С. Г.

Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2023. - 89 с.

Лабораторная работа № 4 «Формирование SIEM-экосистемы»

Цель лабораторной работы №4– Развернуть систему лог-менеджмента AirSIEM (или иную open source SIEM-систему) и разработать в ней дополнительный функционал, позволяющий анализировать регистрируемые в защищаемой инфраструктуре (AirLogger) события, поступающие от различных источников, и обнаруживать атаки/сценарии атак/подозрительные действия/отклонения от нормы, формируя при необходимости соответствующие инциденты безопасности

Задание к лабораторной работе №4:

1) Развернуть систему лог-менеджмента событий безопасности, используя проект AirSIEM (https://github.com/fisher85/AirSIEM). Студент в качестве SIEM-системы вправе использовать иные open source ресурсы (ELK-стэк, Wazuh и т.п. при наличии достаточных системных ресурсов)
2) Реализовать подсистему сбора и хранения поступающих событий безопасности системы AirLogger (или выбранной студентом)
3) Разработать правила корреляции для реализации требований политики ИБ
4) Оформить отчет по лабораторной работе

Структура и форма отчета о лабораторной работе

Отчет по ЛР должен содержать цель и задачи ЛР; скриншоты о процессе развертывания SIEM-системы; результаты эксплуатации развернутой SIEM-системы и результаты срабатывания правил корреляции; выводы по лабораторной работе,

Методические рекомендации по выполнению ЛР приведены в учебном пособии **С. В. Беззатеев, С. Г. Фомичева.** SIEM-системы в управлении информационной безопасностью : учебное пособие / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2021. - 131 с. : рис., табл. - Библиогр.: с. 128- 130 (28 назв.). - ISBN 978-5-8088-1676-3

Лабораторная работа №5 «Управление событиями безопасности»

Цель лабораторной работы №5: Освоить принципы сбора событий безопасности и их анализа правилами корреляции. Освоить принципы построения MVC-решений, позволяющих распределить бизнес-логику в распределенных информационных системах, научиться использовать методы проектирования приложений доступа к данным, базируясь на принципах Model-First и разрабатывать механизмы доступа к хранилищам событий безопасности информации.

Задание лабораторной работы №5:

1) Проверить корректную работоспособность системы лог-менеджмента AirSIEM (или иной SIEM-системы), развернутой в рамках лабораторной работы № 4
2) Изучить материалы лекций по дисциплине «Основы управления информационной безопасностью», размещенные в личном кабинете, а также проверить работоспособность распределенной информационной системы AirLogger, разработанной в качестве объекта защиты. Объект защиты может быть выбран иным (сформированным студентом самостоятельно в рамках ЛР №1-3).
3) В соответствии с заявленной в лекциях функциональностью, разработать Web-клиент, использующий ASP.NET Core MVC подходы разработки распределенных систем. Web-клиент должен обеспечивать возможность удаленного мониторинга таблицы UserExceptions, разработанной ранее архитектуры БД, системы AirLogger, а также поддержку вызова CRUD-операций (create, read, update, delete) над данной таблицей.

4) Локализовать интерфейс Web-клиента (на русском языке должны быть все его элементы)
5) Разработать функционал авторизации пользователей системы AirLogger с ролевой моделью доступа к данным.
6) Разработать дополнительный функционал проекта в соответствии с индивидуальным вариантом.
7) Подключить разработанный web-клиент системы AirLogger в качестве ДОПОЛНИТЕЛЬНОГО источника событий безопасности к системе AirSIEM (событиями безопасности считать добавление данных в таблицу UserExceptions, связанные с нарушением правил политик безопасности при авторизации пользователей).
8) Оформить отчет по лабораторной работе

Структура и форма отчета о лабораторной работе

Отчет по ЛР должен содержать цель и задачи ЛР; скриншоты с результатами работы функционала авторизации пользователей системы AirLogger с ролевой моделью доступа к данным. результаты дополнительного функционала проекта в соответствии с индивидуальным вариантом; выводы по лабораторной работе,

Методические рекомендации по выполнению ЛР приведены в

- учебном пособии **С. В. Беззатеев, С. Г. Фомичева.** SIEM-системы в управлении информационной безопасностью : учебное пособие / С. В. Беззатеев, С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2021. - 131 с. : рис., табл. - Библиогр.: с. 128- 130 (28 назв.). - ISBN 978-5-8088-1676-3
- учебно-методическом пособии **С. Г. Фомичева.** Защита распределенных информационных систем : учебно-методическое пособие / С. Г. Фомичева ; С.-Петерб. гос. ун-т аэрокосм. приборостроения. - Санкт-Петербург : Изд-во ГУАП, 2022. - 55 с. : рис., табл. - Библиогр.: с. 54 (10 назв.).

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;

– 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.

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».

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