



**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ  
РОССИЙСКОЙ ФЕДЕРАЦИИ**

федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ФГБОУ ВО «ИГУ»

**Кафедра радиофизики и радиоэлектроники**



Декан ~~Буднев Н.М.~~

«17» апреля 2024 г.

**Рабочая программа дисциплины (модуля)**

Наименование дисциплины (модуля) **Б1.О.34 Модели информационной безопасности**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **"Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)"**

Квалификация выпускника **-бакалавр**

Форма обучения **очная**

Согласовано с УМК физического факультета

Протокол №42 от «15» апреля 2024 г.

Председатель ~~Буднев Н.М.~~

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8 от «8» апреля 2024 г.

И.О. зав. кафедрой ~~Колесник С.Н.~~

Иркутск 2024 г.

## Содержание

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ.....	3
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО.....	3
3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.....	3
4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ.....	4
4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов.....	4
4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине.....	5
4.3. Содержание учебного материала .....	6
4.3.1. Перечень семинарских, практических занятий и лабораторных работ.....	7
4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СРС).....	7
4.4. Методические указания по организации самостоятельной работы студентов.....	8
4.5. Примерная тематика курсовых работ.....	8
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ .....	9
а) основная литература.....	9
б) дополнительная литература.....	9
в) базы данных, информационно-справочные и поисковые системы.....	9
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ.....	9
6.1. Учебно-лабораторное оборудование.....	9
6.2. Программное обеспечение.....	9
6.3. Технические и электронные средства.....	10
7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ.....	10
8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ.....	11

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Основные цели и задачи, решаемые в ходе преподавания учебной дисциплины, заключаются в формировании у студентов:

- понимание основных рабочих методов моделирования процессов информационной безопасности;
- понимания преимуществ и недостатков различных методов моделирования процессов в информационной безопасности;
- навыка разработки документов исходя из методических материалов ФСТЭК России и ФСБ России;
- навыков моделирования исходя из методики *MITRE* АТТ&СК;
- навыков оценки угроз безопасности информации исходя из регламентирующих документов ФСТЭК России.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Модели информационной безопасности» базируется на дисциплинах «Информатика», «Теория информации».

## 3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **10.03.01 Информационная безопасность**.

### Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
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	Знать: <ul style="list-style-type: none"><li>• основные технологии в автоматизированных системах;</li><li>• регламентирующую документацию ФСТЭК и ФСБ России по моделированию угроз безопасности информации.</li></ul> Уметь: <ul style="list-style-type: none"><li>• проводить анализ угроз безопасности информации, формализовывать результат.</li></ul> Владеть: <ul style="list-style-type: none"><li>• навыками разработки Модели безопасности по различным методикам.</li></ul>

#### 4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 4 зачетные единицы, 144 часов,  
Форма промежуточной аттестации: экзамен

##### 4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/п	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Тема 1.	5	15		6	6		8	Тестовый контроль по теме
2	Тема 2.	5	23		7	7		10	Тестовый контроль по теме
3	Тема 3.	5	23		7	7		10	Тестовый контроль по теме
4	Тема 4.	5	23		7	7		10	Тестовый контроль по теме
5	Тема 5.	5	24		7	7	1	10	Тестовый контроль по теме

#### 4.2. План внеаудиторной самостоятельной работы обучающихся по дисциплине

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
5	Тема 1-3	Подготовка к контрольной работе №1	1-5 неделя	8	Контрольная работа №1	Список дополнительной литературы
5	Тема 1-3	Контрольная работа №1.	6 неделя	10	Контрольная работа №1	Список дополнительной литературы
5	Тема 1-3	Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.	7 неделя	10	Контрольная работа №1	Список дополнительной литературы
5	Тема 4-5	Подготовка к контрольной работе №2	8-15 неделя	10	Контрольная работа №2	Список дополнительной литературы
5	Тема 4-5	Контрольная работа №2.	16 неделя	10	Контрольная работа №2	Список дополнительной литературы

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
Общий объем самостоятельной работы по дисциплине (час)				<b>48</b>		

### 4.3. Содержание учебного материала

#### ***РАЗДЕЛ 1 (Тема 1). ВВЕДЕНИЕ В МОДЕЛИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.***

Ключевые понятие в моделировании. Имитационное моделирование, агентный подход. Событийное моделирование. Динамическое моделирование. Четкая логика. Нечеткая логика. Моделирование на основе сценариев. Риск-ориентированный подход. Необходимые понятия информационной безопасности в моделировании угроз. Основные регламентирующие документы ФСТЭК России и ФСБ России регламентирующие модели в области защиты информации в РФ. Историческая справка.

#### ***РАЗДЕЛ 2 (Тема 2). МОДЕЛИРОВАНИЕ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.***

Модели разграничения доступа. Мандатная модель доступа (Модель Белла — Лападулы). Дискреционная модель доступа. Ролевая модель доступа. Смешанные модели доступа. Методики ФСТЭК России. Методика классификации ФСБ России. Методики классификации ФСТЭК России.

#### ***РАЗДЕЛ 3 (Тема 3). МОДЕЛЬ УГРОЗ.***

Модель угроз ФСБ России (криптография). Модель оценки угроз ФСТЭК России. Источники угроз. Методы реализации угроз. Объекты воздействия. Кorteж описания угрозы. Граница информационной системы.

#### ***РАЗДЕЛ 4 (Тема 4). СЦЕНАРИИ УГРОЗ.***

Сценарии реализации угроз. Тактики. Техники. Примеры типовых оценок угроз. Угрозы безопасности целостности. Угрозы безопасности доступности. Угрозы безопасности конфиденциальности.

#### ***РАЗДЕЛ 5 (Тема 5). MITRE ATT&CK***

Сценарии реализации угроз. Тактики. Техники. Процедуры. Отличия от оценки угроз ФСТЭК России. Программное обеспечение реализации угроз. Нейтрализация угроз безопасности информации. Программное обеспечение нейтрализации угроз. Организационные меры нейтрализации угроз.

#### 4.3.1. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1.	Раздел 2	Лабораторная №1	6		Тестовый контроль по теме	ОПК-10
2.	Раздел 3	Лабораторная №2	7		Тестовый контроль по теме	ОПК-10
3.	Раздел 3	Лабораторная №3	7		Тестовый контроль по теме	ОПК-10
4.	Раздел 4	Лабораторная №4	7		Тестовый контроль по теме	ОПК-10
5.	Раздел 5	Лабораторная №5	7		Тестовый контроль по теме	ОПК-10
6.	Раздел 5	Лабораторная №6	6		Тестовый контроль по теме	ОПК-10

#### 4.3.2. Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СР)

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1.	Тема 1	Контрольная работа №1.	ОПК-10	Способность принимать участие в формировании политики информационной безопасности Способность организовывать, поддерживать и управлять выполнением комплекса мер по обеспечению информационной безопасности
2.	Тема 2	Контрольная работа №1.	ОПК-10	Способность принимать участие в формировании политики



				информационной безопасности Способность организовывать, поддерживать и управлять выполнением комплекса мер по обеспечению информационной безопасности
3.	Тема 3	Контрольная работа №1.	ОПК-10	Способность принимать участие в формировании политики информационной безопасности Способность организовывать, поддерживать и управлять выполнением комплекса мер по обеспечению информационной безопасности
4.	Тема 4	Контрольная работа №2.	ОПК-10	Способность принимать участие в формировании политики информационной безопасности Способность организовывать, поддерживать и управлять выполнением комплекса мер по обеспечению информационной безопасности
5.	Тема 5	Контрольная работа №2.	ОПК-10	Способность принимать участие в формировании политики информационной безопасности Способность организовывать, поддерживать и управлять выполнением комплекса мер по обеспечению информационной безопасности

#### 4.4. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Безопасность информационных технологий», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- подготовка к зачету и экзамену.

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

Каждая лабораторная работа по итогу ее выполнения защищается. В защиту лабораторной работы входят свободно оформленный отчет по проведению работы с зафиксированными ключевыми моментами и результатами работы и вербальное описание хода работы, логики поиска решений и их выполнение.

#### 4.5. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

## **5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **а) основная литература**

1. Федеральный закон от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
3. Приказ ФСТЭК России от 11 февраля 2013 №17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
4. Приказ ФСТЭК России от 29 апреля 2021 №77, «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
5. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
6. Методический документ «Методика оценки угроз безопасности информации» (утв. Федеральной службой по техническому и экспортному контролю 5 февраля 2021 г.);
7. Приказ ФСБ РФ №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», от 9 февраля 2005 (ПКЗ-2005).

### **б) дополнительная литература**

1. Руководство по эксплуатации Metasploit - <https://docs.metasploit.com/>.
2. Руководство по эксплуатации Metasploitable 2  
<https://docs.rapid7.com/metasploit/metasploitable-2>
3. Руководство по эксплуатации Metasploitable 3 -  
<https://github.com/rapid7/metasploitable3>

### **г) базы данных, информационно-справочные и поисковые системы**

1. Открытый проект (OWASP) по Web угрозам - <https://owasp.org/>;
2. Банк данных угроз ФСТЭК России (угрозы) - <https://bdu.fstec.ru/threat>;
3. Банк данных угроз ФСТЭК России (уязвимости) - <https://bdu.fstec.ru/vul>.
4. Открытый проект MITRE ATT&CK <https://attack.mitre.org/resources/getting-started/>

## **6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

### **6.1. Учебно-лабораторное оборудование:**

Компьютерная лаборатория 323б (16 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

### **6.2. Программное обеспечение**

1. Oracle VM VirtualBox 5.0.12. Бессрочно.
2. Microsoft OfficeProPlus 2013 RUS OLP NL Acdmc. Контракт № 03-013-14 от 08.10.2014.Номер Лицензии Microsoft 45936786. Бессрочно.
3. WinPro10 Rus Upgrd OLP NL Acdmc. Сублицензионный договор № 502 от 03.03.2017 Счет № ФРЗ- 0003367 от 03.03.2017 Акт № 4496 от 03.03.2017 Лицензия №

68203568. Бессрочно.

4. Kaspersky Free (ежегодно обновляемое ПО). Условия использования по ссылке: <http://www.kaspersky.ru/free-antivirus/> . Бессрочно.

5. SecretNetStudio 8 (Demo version)

6. Metasploitable 2 (Linux) BSD license

7. Metasploitable 3 (Ubuntu) BSD license

8. Kali Linux, Metasploit 6 GNU GPL.

9. ScanOVAL (ФСТЭК России) Free.

### 6.3. Технические и электронные средства:

В ходе учебного процесса используются технические средства обучения и контроля знаний студентов (презентации, контролирующие программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания.

## 7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для достижения планируемых результатов обучения, в дисциплине «Безопасность информационных технологий» используются различные образовательные технологии:

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

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

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

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

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

**Личностно-ориентированные технологии обучения**, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в

результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

## **8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

### **8.1. Оценочные средства для входного контроля**

Входной контроль (2 варианта, 5-й семестр), представляет собой перечень из 30 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 30 минут. Проверяется уровень входных знаний.

### **8.2. Оценочные средства текущего контроля**

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

### **8.3. Оценочные средства для промежуточной аттестации**

(в форме экзамена).

Тестовые работы. Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

### **Демонстрационный вариант тестовой работы**

**Оценка угроз безопасности информации согласно Методическому документу «Методика оценки угроз безопасности информации» ФСТЭК России.**

1. Напишите 5 сценариев сетевых атак с разложением на техники и тактики до момента закрепления в системе.
2. Напишите 5 техник тактики - «Сбор информации о системах и сетях»

### **ВОПРОСЫ**

#### **Вариант 1**

1. Конфиденциальность информации это:
  - а) свойство безопасности информации быть полученной обладателем информации за приемлемый промежуток времени;
  - б) свойство безопасности информации быть доступной определенному кругу лиц;
  - в) свойство безопасности информации быть неискаженной.
2. Что является главной задачей Модели угроз безопасности информации?
  - а) провести оценку угроз безопасности информации;
  - б) составить список актуальных угроз безопасности информации;
  - в) составить список нарушителей.

3. Угроза это:

- а) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации;
- б) совокупность нарушителя и защищаемой информации.

4. Что такое риск в информационной безопасности?

- а) произведение вероятности реализации угрозы на стоимость ущерба от нее;
- б) произведение вероятности реализации угрозы на стоимость ущерба от неё.

5. Кто является внутренним нарушителем угроз безопасности информации?

- а) разработчик программно-аппаратных средств;
- б) системный администратор;
- в) контрагент организации.

6. Модель Белла — Лападулы описывает

- а) дискреционную модель доступа;
- б) мандатную модель доступа;
- в) ролевую модель доступа;
- г) смешанную модель доступа.

7. Согласно документа «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 5 февраля 2021) внутренний нарушитель имеет больший потенциал, чем внешний?

- а) да;
- б) нет;
- в) потенциал нарушителя не зависит от его отнесения к внешнему или внутреннему.

8. Документ «Методика оценки угроз безопасности информации» (утв. ФСТЭК России 5 февраля 2021) регулирует моделирование угроз в:

- а) информационных системах персональных данных;
- б) государственных и муниципальных информационных системах;
- в) информационных системах обрабатывающих государственную тайну;
- г) для всех перечисленных информационных систем;
- д) автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах,

представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды.

9. Для чего необходимо проводить классификацию информационных систем?

- а) для формализации системы;
- б) для уточнения подхода к дальнейшей защите информационной системы;
- в) для выявления рисков.

10. Контролируемая зона это:

- а) зона в пределах которой ограничено время пребывания лиц;
- б) пространство, где исключено неконтролируемое пребывание лиц, транспортных и технических средств;
- в) это граница территории в собственности обладателя информационной системы.

11. Уязвимость это:

- а) недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации;
- б) ошибка в программном обеспечении или программно-аппаратном обеспечении;
- в) последовательно выполненные действия приводящие к компрометации информационной системы.

12. Согласно 152-ФЗ «О персональных данных» от 27 июля 2007 года ИСПДн это:

- а) информационная система, где осуществляется обработка персональных данных;
- б) совокупность технических средств обработки информации и персонала;
- в) совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств;

13. Перечислите понятия входящие в кортеж описания угрозы

- а) объект атаки;
- б) угроза;
- в) процедура;
- г) нарушитель;
- д) уязвимость;
- е) воздействие НСД.

14. Понятие угрозы исходящей от технического канала утечки информации должно содержать в себе:

- а) понятие среды распространения;
- б) понятие источника сигнала;
- в) понятие приемника сигнала;
- г) только понятие источника сигнала и понятие среды распространения.

15. Что может быть объектом атаки?

- а) алгоритм;
- б) системное программное обеспечение;
- в) аппаратное обеспечение;
- г) все перечисленные варианты.

16. Есть ли понятие вероятности наступления угрозы в подходе « MITRE ATT&CK?»

- а) да;
- б) нет.

17. Какие есть угрозы непосредственного доступа в банке данных угроз ФСТЭК России?

- а) УБИ.004: угроза аппаратного сброса пароля BIOS;
- б) УБИ.099: Угроза обнаружения хостов;
- в) УБИ.100: Угроза обхода некорректно настроенных механизмов аутентификации
- г) УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации.

18. Уязвимость нулевого дня это

- а) уязвимость которая еще не устранена;
- б) уязвимость, которая не известна обладателю информационной системы.

19. Можно ли восстановить конфиденциальность информации?

- а) да;
- б) нет.

20. Какие проекты рассматривают угрозы связанные только с WEB.

- а) банк данных угроз ФСТЭК России;
- б) SAPEC;

в) OWASP;

г) Mitre attack.

21. Какой тип моделирования используется в документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России от 2008 г.)?

а) событийный;

б) имитационный;

в) системно-динамический.

г) агентный.

22. Сколько классов ГИС существует согласно Приказу ФСТЭК России №17?

а) 2;

б) 3;

в) 4.

23. Аутентификация это:

а) действия по проверке подлинности субъекта доступа и/или объекта доступа, а также по проверке принадлежности субъекту доступа и/или объекту доступа предъявленного идентификатора доступа и аутентификационной информации;

б) наделение правами субъекта доступа при входе в информационную систему;

в) выделение субъекта доступа среди других.

24. Каким понятием не оперирует документ «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 14 февраля 2008 г.) ?

а) тактика;

б) процедура;

в) техника.

25. Контроль нарушения каких свойств безопасности информации возможно техническим мерами?

а) целостности;

б) доступности;

в) конфиденциальности.

26. Что такое сценарий исходя из подхода Mitre attack?



- а) изменение характеристик системы во время атаки;
- б) построенный граф перехода информационной системы из одного состояния в другое;
- в) совокупность тактик и техник.

27. Несанкционированный доступ это:

- а) доступ субъекта доступа к объекту доступа, нарушающий правила управления доступом;
- б) нарушение правового режима в информационной системе;

28. Целостность информации это:

- а) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- а) свойство информационной системы противостоять несанкционированному искажению информации.

29. Расположите классы криптографической защиты с возрастанием требований:

- а) КС1,КС2,КС3;
- б) КС3,КС2,КС1.

30. Что относится к угрозам сетевого характера согласно банку данных угроз ФСТЭК России?

- а) УБИ.006: Угроза внедрения кода или данных;
- б) УБИ.069: Угроза неправомерных действий в каналах связи;
- в) УБИ.099: Угроза обнаружения хостов

Вариант 2

1. Модель Белла — Лападулы описывает

- а) дискреционную модель доступа;
- б) мандатную модель доступа;
- в) ролевую модель доступа;
- г) смешанную модель доступа.

2. Контроль нарушения каких свойств безопасности информации возможно техническим мерами?

- а) целостности;
- б) доступности;

в) конфиденциальности.

3. Что такое сценарий исходя из подхода Mitre attack?

- а) изменение характеристик системы во время атаки;
- б) построенный граф перехода информационной системы из одного состояние в другое;
- в) совокупность тактик и техник.

4. Целостность информации это:

- а) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;
- а) свойство информационной системы противостоять несанкционированному искажению информации.

5. Перечислите понятия входящие в кортеж описания угрозы:

- а) объект атаки;
- б) угроза;
- в) процедура;
- г) нарушитель;
- д) уязвимость;
- е) воздействие НСД.

6. Какие проекты рассматривают угрозы связанные только с WEB.

- а) банк данных угроз ФСТЭК России;
- б) CAPEC;
- в) OWASP;
- г) Mitre attack.

7. Сколько классов ГИС существует согласно Приказу ФСТЭК России №17.

- а) 2;
- б) 3;
- в) 4.

8. Сколько примерно угроз содержится в банке данных угроз ФСТЭК России?

- а) 220;
- б) 550;

в) 50.

9. Для каких угроз важно расположение информационной системы относительно контролируемой зоны?

- а) для угроз связанных с техническими каналами;
- б) для угроз связанных с программным обеспечением;
- в) для всех перечисленных.

10. Исходя из каких документов будет разрабатываться Модель угроз для ИСПДн?

- а) Постановление Правительства РФ от 1 ноября 2012 г. №1119;
- б) Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. ФСТЭК России 14 февраля 2008 г.);
- в) Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России от 2008 г.)?

11. Расположите уровни компетенции нарушителей в порядке их возрастания:

- а) Н1, Н2, Н3,Н4;
- б) Н4,Н3,Н2,Н1.

12. Сколько тактик нарушителя предлагается в проекте Mitre attack?

- а) 14;
- б) 10.

13. Согласно методического документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России от 2008 г.)? бывшие работники организации относятся к какому типу нарушителей?

- а) внутренний;
- б) внешний.

14. Какие понятия есть в документе «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России 14 февраля 2008 г.)?

- а) перечень возможных (вероятных) угроз безопасности информации для соответствующих способов их реализации и уровней возможностей нарушителей;
- б) сценарий реализации угрозы;
- в) актуальность угрозы.

15. Доступность информации это

- а) возможность получить информацию;
- б) свойство безопасности информации в получении последней за приемлемый промежуток времени.

16. Конфиденциальность это:

- а) субъективное понятие;
- б) объективное понятие.

17. Сколько типов нарушителя предлагается в документе «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (утв. ФСТЭК России от 2008)?

- а) 3;
- б) 7.

18. Какие техники применяются в начале атаки?

- а) направленное сканирование с помощью специализированного ПО;
- б) сбор информации о пользователе;
- в) модификация модулей и конфигурации вредоносного ПО.

19. Какое мероприятие позволяет контролировать целостность ПО?

- а) вычисление контрольных сумм защищаемых файлов (криптографическое преобразование);
- б) создание резервных копий защищаемых файлов.

20. Какие объекты информатизации предусмотрены документами ФСТЭК относятся ПЭВМ?

- а) АРМ;
- б) ЗП;
- в) ВП.

21. Недекларированные возможности (НДВ) это:

- а) функциональные возможности программного обеспечения, не описанные в документации;
- б) возможности при помощи которых можно совершить НСД.

22. Что относится к основным объектам атаки при межсетевом взаимодействии?

- а) операционная система;
- б) коммутаторы;
- в) сетевые сервисы.

23. Что необходимо для правового обоснования защиты информации на объекте от разглашения и несанкционированного доступа?

- а) перечень лиц, допущенных до обработки конфиденциальной информации;
- б) перечень программного обеспечения на объекте;
- в) согласие о неразглашении...;

24. Кто несет ответственность за защиту информации в организации при отсутствии организационно-распорядительной документации?

- а) руководитель организации;
- б) системный администратор;
- в) пользователи.

25. Техническая защита информации это:

а) защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств;

б) а) защита информации, заключающаяся в обеспечении любыми методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

26. Какие технические средства позволяют контролировать утечку информации?

- а) COB;
- б) DLP;
- в) МЭ.

27. Согласно проекту Mitre attack что означает ICS?

- а) общий раздел описания тактик и техник;
- б) раздел угроз мобильных приложений;
- в) раздел описания тактик и техник систем промышленной автоматизации.

28. Системный администратор допущенный до обработки конфиденциальной информации является нарушителем?

а) да;

б) нет.

29. Какие существуют средства защиты от угроз загрузки с внешних носителей?

а) средства доверенной загрузки;

б) антивирусное ПО;

в) криптографические методы.

30. Что такое аттестация объектов информатизации?

а) комплекс мер направленный на защиту информации;

б) совокупность специальной проверки и специального исследования;

в) комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных ФСТЭК России.

**Разработчик:**



преподаватель А.Л.Горбылев

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

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «8» апреля 2024 г. Протокол № 8

И.О. зав. кафедрой  Колесник С.Н.

*Настоящая программа, не может быть воспроизведена ни в какой форме без предварительного письменного разрешения кафедры-разработчика программы.*