МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.В.04 Математические модели политики информационной безопасности**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

Направленность (профиль) подготовки №4 Безопасность автоматизированных систем (в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

1. Цели и задачи дисциплины (модуля)

Дисциплина «Математические модели и политики информационной безопасности», как дисциплина профессионального цикла направлена на достижение следующих целей:

• подготовку специалистов к деятельности, связанной с моделированием угроз безопасности информации и разработки моделей угроз.

Для достижения поставленной цели сформулированы следующие задачи:

• овладение основами методиками моделирования;

• изучение принципов построения моделей в информационной безопасности;

• изучение методического опыта моделирования в РФ и зарубежных подходов моделирования;

• овладение программными средствами моделирования угроз безопасности информации.

2. Место дисциплины в структуре ОПОП

Дисциплине опирается на знания, полученные в ходе изучения дисциплин «Информатика» и «Теория информации», которые должны быть освоена полностью и студенты должны владеть навыками работы на ПЭВМ.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

ОПК-10 - Способность принимать участие в формировании политики информационной безопасности. Способность организовывать, поддерживать и управлять выполнением комплекса мер по обеспечению информационной безопасности

В результате изучения дисциплины студент должен:

Знать:

- историю развития подходов к моделированию;
- классификацию подходов моделирования угроз безопасности информации;
- преимущества и недостатки различных методов моделирования;
- организационно-правовую основу в РФ;

Уметь:

- формализовать поставленную задачу;
- применять полученные знания в моделировании угроз безопасности;
- ориентироваться в правовой базе по моделированию;
- использовать действующие методики моделирования.

Владеть:

- навыками разработки моделей угроз для различных информационных систем.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	**Всего часов / зачетных единиц**	**Семестры**			
		5			
Аудиторные занятия (всего)	118/3,27	118/3,27			
В том числе:	-	-	-	-	-
Лекции	50/1,38	40/1,38			
Практические занятия (ПЗ)	34/0,94	34/0,94			
Семинары (С)					
Лабораторные работы (ЛР)	34/0,94	34/0,94			
КСР					
Самостоятельная работа (всего)	134/3,72	134/3,72			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	134/3,72	134/3,72			
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	118/3,27	118/3,27			
Общая трудоемкость часы	252	252			
зачетные единицы	7	7			

5. Содержание дисциплины (модуля)

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

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 защити 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. Кортеж 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.

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Радиотехнические цепи и сигналы	1-5
2	Защита информации от несанкционированного доступа	1-5
3	Электроника и схемотехника	1-5
4	Операционные системы	1-5
5	Базы данных	1-5
6	Безопасность компьютерных сетей	1-5
7	Практика по получению первичных профессиональных умений и навыков	1-5

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1	10	6		2	30	48
2.	***Раздел 2***	Тема 2	10	7		8	26	51
3.	***Раздел 3***	Тема 3	10	7		8	26	51
4.	***Раздел 4***	Тема 4	10	7		8	26	51
5.	***Раздел 5***	Тема 5	10	7		8	26	51

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1***	Лабораторная №1	2	Тестовый контроль по теме	ОПК-10
2.	***Раздел 2***	Лабораторная №2	8	Тестовый контроль по теме	ОПК-10
3.	***Раздел 3***	Лабораторная №3	8	Тестовый контроль по теме	ОПК-10
4.	***Раздел 4***	Лабораторная №4	8	Тестовый контроль по теме	ОПК-10
5.	***Раздел 5***	Лабораторная №5	4	Тестовый контроль по теме	ОПК-10
7.	***Раздел 5***	Лабораторная №6	4	Тестовый контроль по теме	ОПК-10

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-3**	Подготовка к контрольной работе №1	№1	Учебный сайт	64
8		Контрольная работа №1.		Учебный сайт	2
9		Подведение итогов по контрольной		Учебный сайт	1

		работе №1. Работа над ошибками по контрольной работе №1.			
10-15	**4-5**	Подготовка к контрольной работе №2.	№2	Учебный сайт	64
16		Контрольная работа №2.		Учебный сайт	3

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Математические модели и политики информационной безопасности», 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;
- выполнение индивидуальных проектов;
- подготовка к контрольным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Математические модели и политики информационной безопасности», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

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

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать условия для выполнения самостоятельной работы (учебно-методическое обеспечение),

правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

- Федеральный закон от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
- Приказ ФСТЭК России от 11 февраля 2013 №17 «Об утверждении требований о защите информации , не составляющей государственную тайну, содержащейся в государственных информационных системах»;
- 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»;
- 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»;
- Базовая модель угроз безопасности персональных дынных. ФСТЭК России от 2008 г.;
- 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

- Руководство по эксплуатации Metasloit - https://docs.metasploit.com/.
- Руководство по эксплуатации Metasloitable 2 https://docs.rapid7.com/metasploit/metasploitable-2
- Руководство по эксплуатации Metasloitable 3 - https://github.com/rapid7/metasploitable3

г) базы данных, информационно-справочные и поисковые системы

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

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 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.

10. Образовательные технологии

Для достижения планируемых результатов обучения, в дисциплине «Математические модели и политики информационной безопасности» используются различные образовательные технологии:

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

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

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

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

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

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых

условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

Входной контроль (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.

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (5 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

11.3. Оценочные средства для промежуточной аттестации

(в форме зачета).

Тестовые работы (2 варианта). Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

ВОПРОСЫ

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. Кофиденциальность 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) CAPEC;

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. Аутетнификация 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 состояние 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 относиться 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) обьективное 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 предусмотреные 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 относиться к основным обьектам 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) СОВ;

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) антивирсное ПО;

в) криптографические методы.

30. Что такое аттестация объектов информатизации?

а) комплекс мер направленный на защиту информации;

б) совокупность спецаильной 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 рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

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