	МИНОБРНАУКИ РОССИИ
	ФГБОУ ВО «Амурский государственный университет»
	Факультет математики и информатики
	Кафедра информационной безопасности

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

по компетенции ОПК – 1

Направление подготовки 10.03.01 – Информационная безопасность

Направленность (профиль) образовательной программы
Безопасность автоматизированных систем
(по отрасли или в сфере профессиональной деятельности)

Квалификация выпускника – бакалавр

Благовещенск 2023 г.

Основы информационной безопасности

1 «Под информационной безопасностью будем понимать защищенность информации и поддерживающей _____ от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры»

Ответ: инфраструктуры

2. Возможность за приемлемое время получить требуемую информационную услугу называется _____

Ответ: доступность

3.Установление подлинности идентифицированного пользователя – это _____.

Ответ: аутентификация

4. Полномочия, устанавливаемые администратором системы для конкретных лиц, позволяющие последним использовать информацию, файлы или всю систему в целом – это _____

Ответ: авторизация

5. _____ сеть компьютеров, зараженных вредоносной программой, позволяющей киберпреступникам удаленно управлять зараженными машинами без ведома пользователя, которая чаще всего используются хакерами для организации DDoS-атак и массовой спам-рассылки.

Ответ: ботнет

6. При выборе системы защиты необходимо найти компромисс между _____ на защиту информационных объектов и возможными потерями при реализации информационных угроз

Ответ: затратами

7. Попытка реализации угрозы – это **_____**

Ответ: атака

8. Социальная _____ или «атака на человека» — это совокупность психологических и социологических приёмов, методов и технологий, которые позволяют получить конфиденциальную информацию.

Ответ: инженерия

9. _____ – это процедура опознавания пользователя по предъявленному идентификатору.

Ответ: идентификация

10. Вирус поражающий документы называется _____

Ответ: макровирус

11. Потенциальная возможность определенным образом нарушить информационную безопасность–это _____**.**

Ответ: угроза

12. Основополагающим документом в РФ является _____

Ответ: Конституция РФ

13. Дублирование сообщения является угрозой _____

Ответ: целостности

14. Перехват данных является угрозой _____

Ответ: конфиденциальности

15. «_____письма» – вид мошенничества, когда у получателя писем просят помощи в обналичивании крупной суммы денег, и получивший наибольшее развитие с появлением массовых рассылок по электронной почте (спама).

Ответ: Нигерийские

16._____имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом.

Ответ: Каждый

17. Информация – наиболее ценный _____современного общества

Ответ: ресурс

18. война – это война без правил, война без видимых разрушений и порой даже без четко определенного противника.

Ответ: Информационная

19. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Ответ: личности

20. _____ – вид интернет-мошенничества, когда распространяются поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей**.** Чаще всего зло-

умышленники выдают себя за представителей известных организаций в электронных письмах или телефонных звонках.
Ответ: Фишинг

21. Тип атаки, направленной для ограничения или полного прекращения доступа пользователей к компьютерной системе - атака «_____в обслуживании»

Ответ: отказ

22. Меры информационной безопасности направлены на защиту от нанесения неприемлемого _____
Ответ: ущерба

23. Комплекс мероприятий направленных на обеспечение информационной безопасности называется _____информации.
Ответ: защитой

24. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:

1. детектор
2. доктор
3. сканер
4. ревизор
5. сторож
6. посетитель

Ответ: 2

25. П**рограмма с вредоносным кодом, которая атакует компьютеры в сети и распространяется через нее, называется:**

1. компаньон - вирусами
2. черви
3. паразитические
4. студенческие
5. стелс - вирусы
6. макровирусы

Ответ: 2

26. **Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:**

1. Принцип системности
2. Принцип комплексности
3. Принцип непрерывной защиты
4. Принцип разумной достаточности
5. Принцип гибкости системы

6. Принцип обоснованности доступа

Ответ: 3

27. Процесс, при котором злоумышленник может получить доступ к объектам, удаленным другими пользователями, просмотрев содержимое их корзин, называется

1. методом грубой силы
2. сканированием
3. уборка "мусора"
4. агрегированием
5. спуфер
6. маскарад

Ответ: 3

28. Естественные угрозы безопасности информации вызваны:

1. деятельностью человека
2. ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения
3. воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека
4. подслушивание переговоров
5. ошибками при действиях персонала
6. хакерские атаки

Ответ: 3

29. Уровень защиты информационной системы определяется

1. степенью защиты ее самого надежного звена
2. степенью защиты ее самого уязвимого звена
3. средней защищенностью ее компонентов
4. администратором системы
5. степенью защиты ее программного обеспечения
6. пользователем системы

Ответ: 2

30. **Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это**….

1. информационная война
2. информационное оружие
3. информационное превосходство
4. информационное воздействие
5. информационное преступление
6. информационный захват

Ответ: 1

Гуманитарные аспекты информационной безопасности

1. Как называется противоборство сторон посредством распространения специально подготовленной информации и противодействия аналогичному внешнему воздействию на себя?

а) информационная война;

б) конфликт;

в) открытый конфликт;

г) эскалация конфликта;

д) «холодная война»;

е) терроризм.

Ответ: а

2. Что входит в информационную безопасность?

а) открытость, конфиденциальность и целостность информационных ресурсов и поддерживающей инфраструктуры;

б) открытость и конфиденциальность информационных ресурсов и поддерживающей инфраструктуры;

в) конфиденциальность и целостность информационных ресурсов и поддерживающей инфраструктуры;

г) открытость и целостность информационных ресурсов и поддерживающей инфраструктуры;

д) открытость, структурированность, конфиденциальность и целостность информационных ресурсов и поддерживающей инфраструктуры;

е) конфиденциальность, структурированность и целостность информационных ресурсов и поддерживающей инфраструктуры;

Ответ: а

3. Как называется психологическое воздействие на кого-либо с целью возбуждения у него намерений, не совпадающих с его реально существующими желаниями, целями?

а) убеждение;

б) манипулирование;

в) внушение;

г) давление;

д) просьба;

е) разъяснение.

Ответ: б

4. Одним из методов защиты информации от уничтожения или повреждения является:

а) сжатие информации с помощью программ-архиваторов;

б) дефрагментация дисков, на которых хранится информация;

в) ограничение доступа к информации с помощью парольной защиты;

г) криптографическое шифрование информации;

д) копирование конфиденциальной информации;

е) постоянное использование антивирусных программ.

Ответ: в

5. Какая форма информационной войны нацелена на каналы связи между командованием и исполнителями?

а) кибервойна;

б) психологическая;

в) командно-управленческая;
г) хакерская;
д) экономическая;
е) электронная.
Ответ: в

6. Какая форма информационной войны подразумевает диверсионные действия против гражданских объектов противника и защиту от них (например, взлом банковских сетей)?
а) психологическая;
б) экономическая;
в) электронная;
г) хакерская;
д) командно-управленческая;
е) экономическая электронная война.
Ответ: г

7. Информация, которая содержит сведения, составляющие государственную и другую предусмотренную законом тайну, разглашение которой наносит ущерб личности, обществу и государству – это …
а) тайная информация;
б) открытая информация;
в) конфиденциальная информация;
г) государственная информация;
д) общественная информация;
е) секретная информация.
Ответ: а

8. Криптография - это наука, изучающая вопросы:
а) обеспечения секретности передаваемых сообщений с использованием различных методов;
б) техники безопасности при работе с компьютером;
в) шифрования информации;
г) организации защиты информации физическими методами;
д) защиты информации от вирусов;
е) способы хранения информации.
Ответ: а

9. Экономическая информационная война (Economic Info-Warfare) имеет две формы: _____ _____ (направленная против США) и _____ _____ (метод самих США).
Ответ: Экономическая информационная война (Economic Info-Warfare) имеет две формы: **информационная блокада** (направленная против США) и **информационный империализм** (метод самих США).

10. Психологическая борьба подразумевает использование методов информационного противостояния против не информационных систем противника, а непосредственно человеческого разума и психики; выступает как манипулирование _____ _____, _____ _____ на различных социальных уровнях.
Ответ: Психологическая борьба подразумевает использование методов информационного противостояния против не информационных систем противника, а непосред-

ственно человеческого разума и психики; выступает как **манипулирование общественным сознанием**, **общественным мнением** на различных социальных уровнях.

11. _____ _____ представляет собой прикладной метод ведения информационного противостояния, целью которой является снижение информационных возможностей противника (ее разновидности - радиоэлектронная борьба (РЭБ), криптографическая борьба (искажение и ликвидация собственно информации), борьба с коммуникационными системами противника)

Ответ: **Электронная борьба** представляет собой прикладной метод ведения информационного противостояния, целью которой является снижение информационных возможностей противника (ее разновидности - радиоэлектронная борьба (РЭБ), криптографическая борьба (искажение и ликвидация собственно информации), борьба с коммуникационными системами противника).

12. Самой масштабной и опасной по праву считается _____ война.

Ответ: Самой масштабной и опасной по праву считается **психологическая** война.

13. При работе в Интернете рекомендуется пользоваться **_____.**

Ответ: При работе в Интернете рекомендуется пользоваться **паролями.**

14. Продукт современной операции _____-_____ войны -- это сводка новостей СМИ в формате журналистского репортажа, в силу чего происходит формирование нужного общественного мнения.

Ответ: Продукт современной операции **информационно-психологической** войны – это сводка новостей СМИ в формате журналистского репортажа, в силу чего происходит формирование нужного общественного мнения.

15. _____, _____, _____ являются свойствами информационной безопасности.

Ответ: **Конфиденциальность, целостность, доступность** являются свойствами информационной безопасности.

16. Психологическая война оказывает **_____** воздействие на широкие круги общественности.

Ответ: Психологическая война оказывает **информационное** воздействие на широкие круги общественности.

17. Носителями угроз информационной безопасности является _____ _____.

Ответ: Носителями угроз безопасности информации являются **источники угроз**.

18. К основным объектам безопасности относятся _____ , _____ , _____ .

Ответ: К основным объектам безопасности относятся: **личность**; **общество**; **государство**.

19. **_____** - **_____** война нацелена на каналы связи между командованием и исполнителями.

Ответ: **Командно-управленческая** война нацелена на каналы связи между командованием и исполнителями.

20. Основными составляющими информационной безопасности являются _____, _____, _____.

Ответ: Основными составляющими информационной безопасности являются **кон-**

фиденциальность, целостность и доступность.

21. Цель кибервойны - осуществление _____ терроризма (захват компьютерных данных, позволяющих выследить цель либо шантажировать её).

Ответ: Цель кибервойны - осуществление **информационного** терроризма (захват компьютерных данных, позволяющих выследить цель либо шантажировать её).

22. Информационно-психологическая война – это боевые действия, спланированные в соответствии с _____-_____, цель которых – не уничтожение живой силы и техники противника, а достижение определенного _____-_____.

Ответ: Информационно-психологическая война – это боевые действия, спланированные в соответствии с **пиар-сценарием,** цель которых – не уничтожение живой силы и техники противника, а достижение определенного **пиар-эффекта.**

23. Непреднамеренные угрозы возникают в результате действий, совершенных из-за недостатка _____ или по _____.

Ответ: Непреднамеренные угрозы возникают в результате действий, совершенных из-за недостатка **компетентности** или по **неосторожности**.

24. Информационная безопасность – это защищенность _____ _____, а также защита _____ _____ и _____ в информационной сфере.

Ответ: Информационная безопасность – это защищенность **информационных ресурсов**, а также защита **прав личности** и **государства** в информационной сфере.

25. _____ – это такие угрозы информационной безопасности, которые возникают без помощи человека: пожар, наводнение, землетрясение, ураган и др.

Ответ: **Естественные** – это такие угрозы информационной безопасности, которые возникают без помощи человека: пожар, наводнение, землетрясение, ураган и др.

26. _____ – это такие угрозы информационной безопасности, которые возникают только при взаимодействии с человеком.

Ответ: **Искусственные** – это такие угрозы информационной безопасности, которые возникают только при взаимодействии с человеком

27. Система безопасности должна в первую очередь гарантировать _____ и _____информации, а затем уже (если необходимо) ее _____.

Ответ: Система безопасности должна в первую очередь гарантировать **доступность** и **целостность** информации, а затем уже (если необходимо) ее **конфиденциальность.**

28. К преднамеренным угрозам относят действия _____, _____ атаки, _____ обиженных работников и т. д.

Ответ: К преднамеренным угрозам относят действия **конкурентов**, **хакерские** атаки, **вредительство** обиженных работников и т. д.

29. Информационная война рассматривается как способ воздействия на информационное пространство противостоящей стороны с целью достижения стратегических целей, а в ее основе лежит _____ .

Ответ: Информационная война рассматривается как способ воздействия на информационное пространство противостоящей стороны с целью достижения стратегических целей, а в ее основе лежит **пропаганда.**

30. Целью психологической войны профессор В.С. Шатило считает «воздействие на _____ _____ таким образом, чтобы _____ людьми, _____ их действовать против своих интересов.

Ответ: Целью психологической войны профессор В.С. Шатило считает «воздействие на **общественное сознание** таким образом, чтобы **управлять** людьми, **заставить** их действовать против своих интересов.

Введение в профессию

1. Все информационные ресурсы делятся на _____ и _____

Ответ: Общедоступные и конфиденциальные

2. В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг., принятой 9 мая 2017 года дано определение «сертифицированные на соответствие требованиям к ИБ, устанавливаемым федеральным органом исполнительной власти и другими уполномоченными структурами – это _____»

Ответ: безопасные ПО и сервис

3. В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг., принятой 9 мая 2017 года дано определение «концепция компьютерных сетей, соединяющая физические объекты управления (вещи), оснащенные встроенными ИТ для взаимодействия друг с другом или с внешней средой без участия человека – это _____»

Ответ: Интернет вещей

4. В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг., принятой 9 мая 2017 года дано определение «совокупность информационных ресурсов, созданных субъектами информационной среды, средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры – это _____»

Ответ: Информационное пространство

5. В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг., принятой 9 мая 2017 года дано определение «совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи (коммуникационная инфраструктура), используемых для организации ее объектов между собой – это _____»

Ответ: Критическая информационная инфраструктура РФ

6. В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг., принятой 9 мая 2017 года дано определение «информационно-технологическая модель обеспечения повсеместного и удобного доступа в сети Интернет к общему набору конфигурируемых вычислитель-

ных ресурсов, устройствам хранения данных, приложениям и сервисам, которые могут быть оперативно предоставлены и освобождены от нагрузки с минимальными эксплуатационными издержками или без участия провайдера – это _____»
Ответ: Облачные вычисления

7. В Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 гг., принятой 9 мая 2017 года дано определение «информационно-технологическая модель системного уровня для расширения облачных функций хранения, вычисления и сетевого взаимодействия, в которой обработка данных осуществляется на конечном оборудовании в сети – это _____»
Ответ: Туманные вычисления

8. Облачные вычисления принципиально отличаются от туманных –
А) местом обработки данных
Б) функциональными возможностями
В) скоростью обработки данных
Г) отсутствием ИТ-модели
Д) наличием ИТ-модели
Е) нет принципиальных отличий
Ответ: А

9. Системы, отражающие реальность действительности, объективный мир, называются _____
А) Естественные
Б) Искусственные
В) Идеальные
Г) Рефлексивные
Д) нерефлексивные
Е) гомогенные
Ответ: В

10. Простые по структуре, однозначно реагирующие на воздействие внешней среды – …… системы
А) Функциональные
Б) Искусственные
В) Идеальные
Г) Рефлексивные
Д) нерефлексивные
Е) Естественные
Ответ: Г

11. Характеристика целостности системы, описывает ее способность поддерживать свое нормальное функционирование (состояние) в условиях внешних

и внутренних воздействий – это _____
Ответ: Внутренняя безопасность

12. Устойчивое функционирование системы и достижение общей цели – это _____
Ответ: Гомеостаз

13. Способность системы взаимодействовать со средой без нарушения ее (среды) гомеостаза – это _____
Ответ: Внешняя безопасность

14. Сочетание вероятности угрозы разрушения системы и серьезности этой угрозы - _____
Ответ: Риск

15. Отказ, проявляющийся вполне определенным образом по определенной причине, от которой можно избавиться только изменением конструкции, технологических процедур, документации или других определяющих факторов.
Ответ: Системный отказ

16. Вероятность того, что система, включая персонал, будет выполнять требуемые функции при всех предопределенных условиях в течение установленного интервала времени – это _____
Ответ: надежность

17. К наиболее значимым объектам информационной коммуникации с точки зрения безопасности относятся несанкционированные регистраторы передаваемых данных (шпионы) и _____
Ответ: источники помех (помехи, шумы)

18. Утверждение, заведомо не соответствующее действительности и высказанное в таком виде сознательно – это _____
Ответ: ложь

19. Заведомо ложная информация, предоставляемая противнику или деловому партнеру для более эффективного ведения боевых действий, сотрудничества, проверки на утечку информации и направление её утечки, выявление потенциальных клиентов «черного рынка» - это _____
Ответ: дезинормация

20. Информация стареет: оперативно-тактические данные теряют свою ценность по __% в день.
Ответ: 10

21. Мероприятия по защите информации, проведение которых не требует применения специально разработанных технических средств – это _____ мероприятия.
Ответ: Организационные

22. Организационное обеспечение ИБ в ключевых позициях имеет ____ основных класса задач
А) 3
Б) 5
В) 4
Г) 10
Д) 6
Е) 2
Ответ: В

23. Совокупность правил по обеспечению ИБ – это _____ИБ
Ответ: политика

24. Занимается сбором информации о ноу-хау _____ разведка
Ответ: Промышленная

25. Логическим приемником Комитета государственной безопасности СССР стала _____
А) КГБ
Б) Смерш
В) НКВД
Г) ГРУ
Д) СВР
Е) Министерство обороны РФ
Ответ: Д

26. Центральный орган управления военной разведкой в Вооружённых Силах РФ – это _____
А) КГБ
Б) Смерш
В) НКВД
Г) ГРУ
Д) СВР
Е) Министерство обороны РФ
Ответ: Г

27. Управление «…» — подразделение МВД РФ, осуществляет борьбу с преступлениями в сфере ИТ.
Ответ: К

28. Нарушение действующего законодательства с использованием ИТ-устройств и процессов, с целью НСД (считывание, искажение, уничтожение данных) к информации – это _____.
Ответ: киберпреступление

29. Какой способ начала кибератаки самый распространенный в настоящее время?
Ответ: Фишинг

30. Какую из задач помогают решить алгоритмы симметричного шифрования?
А) Доступность
Б) Конфиденциальность
В) Аутентичность
Г) Неотрицание авторства
Д) Полезность
Е) Обладание и контроль
Ответ: Б