Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 11.04.2023 12:46:13
Уникальный программный ключ:
0b817ca911e6668abb13a5d426d39e5f1c11eabbf73e943df4a4851fda56d089

МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

УТВЕРЖДАЮ:
Заведующий кафедрой
информационной безопасности
(наименование ф-та полностью)
М.О. Таныгин
(подпись, инициалы, фамилия)
« 29 » августа 2022 г.

ОЦЕНОЧНЫЕ СРЕДСТВА
для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Гуманитарные аспекты информационной безопасности
(наименование учебной дисциплины)

10.03.01 Информационная безопасность, профиль Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий

(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ УСТНОГО ОПРОСА

Тема 1. Доктрина информационной безопасности Российской Федерации: аналитический обзор

1. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?
2. Как называется состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?
3. Как называется состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно?
4. Перечислите основные социальные сферы, в которых предполагается обеспечение информационной безопасности.
5. Перечислите объекты информатизации, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий.

Тема 2. Безопасность личности, общества и государства: дифференциация и взаимосвязь уровней информационной безопасности

1. Меры информационной безопасности направлены на защиту от?
2. Что такое защита информации?
3. Что понимается под информационной безопасностью?
4. Опишите концепцию сообщества безопасности.
5. Перечислите уровни информационной безопасности.

Тема 3. Объективные и субъективные аспекты Информационной безопасности в условиях Социальной турбулентности

1. "Информационная безопасность" – это?
2. Информационная безопасность предполагает?
3. Менеджмент в сфере информационной безопасности включает в себя?
4. Перечислите когнитивные аспекты восприятия.
5. Дайте понятие социальной турбулентности.

Тема 4. Экзистенциально-личностное измерение безопасности и информационная безопасность личности, духовная безопасность личности

1. Какой закон регулирует отношения, связанные с защитой детей от травмирующего их психику информационного воздействия, жестокости и насилия в общедоступных СМИ?
2. Какой термин соответствует состоянию защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их

здоровью и (или) физическому, психическому, духовному, нравственному развитию?

3. Какой закон ввел обязанность владельцев интернет-сайтов удалить интернет-страницу, на которой размещается запрещенная к распространению информация, после получения соответствующего уведомления от хостинг-провайдера?

4. Что является фундаментальными условиями трансформации человека как социокультурного и природного существа?

5. Что такое динамическая адаптации к меняющимся условиям?

Тема 5. Цивилизационные аспекты национально-информационной безопасности

1. К какому уровню обеспечения ИБ относится «Доктрина информационной безопасности Российской Федерации»?

2. К какому уровню обеспечения ИБ относятся действия общего и специального характера, предпринимаемые руководством организации?

3. Перечислите проблемы онтологичности социального бытия.

4. В чем заключается проблема экспликации параметров выстраивания стратегии безопасности?

5. Перечислите основные аспекты ИБ.

Тема 6. Виртуальные девиантные сообщества и деструктивный контент социальных сетей

1. К какому уровню обеспечения ИБ относятся меры безопасности, закрепленные в соответствующих методологиях и реализуемые ответственными менеджерами и персоналом предприятия?

2. К какому уровню обеспечения ИБ относятся конкретные методики, программно-аппаратные, технологические и технические меры?

3. К какому уровню обеспечения ИБ относится «Политика информационной безопасности», утвержденная руководителем в конкретной организации?

4. Дайте понятие термина «информационная война».

5. Что такое «деструктивный контент»?

Критерии оценки:

4-3 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий;

недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Контрольные вопросы к практической работе №1 «Организационные и правовые основы обеспечения безопасности персональных данных»:

1. Перечислите виды защищаемых персональных данных.
2. Дайте правовую характеристику личной тайне.
3. В чём заключается сущность правовой защиты различных видов тайн?
4. Чем вызвана необходимость правовой защиты различных видов тайн?
5. Оцените надёжность правовой защиты различных видов тайн.
6. Укажите принципиальные различия между различными видами тайн и персональными данными.
7. Составьте перечень личных тайн.
8. Сравните различные виды персональных данных с точки зрения правовой защиты.

Контрольные вопросы к практической работе №2 «Уголовная ответственность за правонарушения в сфере информационной безопасности»:

1. Дайте определение понятию «разглашение защищаемой информации».
2. Перечислите виды разглашаемой информации.
3. Дайте характеристику уголовно-правовым способам борьбы с разглашением защищаемой информации.
4. От чего зависит применение уголовно-правовых норм в борьбе с разглашением защищаемой информации?
5. Укажите состав уголовного правонарушения при применении норм в борьбе с разглашением защищаемой информации.
6. Каковы существенные особенности правил защиты информации?
7. Приведите пример применения уголовных норм в борьбе с разглашением защищаемой информации.
8. Составьте перечень норм публичного права, направленных на борьбу с разглашением защищаемой информации.
9. Сравните зарубежный опыт борьбы с разглашением защищаемой информации с российским опытом.

Контрольные вопросы к практической работе №3 «Гражданская и дисциплинарная ответственность за правонарушения в сфере информационной безопасности»

1. Дайте характеристику гражданско-правовому способу защиты охраняемой информации.

2. Перечислите виды гражданско-правовых норм, направленных на защиту охраняемой информации.

3. Дайте определение понятию «защита охраняемой информации».

4. Обоснуйте место гражданско-правового способа защитыохраняемой информации в российском праве.

5. Каковы существенные особенности защиты охраняемой информации при помощи гражданско-правовых норм права?

6. Укажите принципиальные различия защиты охраняемой информации при помощи гражданско-правовых норм права.

7. Приведите примеры защиты охраняемой информации при помощи гражданско-правовых норм права.

8. Составьте перечень гражданско-правовых норм, направленных на защиту охраняемой информации.

9. Сравните зарубежный опыт защиты охраняемой информации при помощи гражданско-правовых норм права.

Контрольные вопросы к практической работе №4 «Административная ответственность за правонарушения в сфереинформационной безопасности»

1. Дайте определение понятию «разглашение защищаемой информации».

2. Перечислите виды разглашаемой информации.

3. Обоснуйте значение административно-правовых способов борьбы с разглашением защищаемой информации.

4. От чего зависит применение уголовно-правовых или административно-правовых норм в борьбе с разглашением защищаемой информации?

5. Укажите состав административного правонарушения при применении норм в борьбе с разглашением защищаемой информации.

6. Каковы существенные особенности правил защиты информации?

7. Приведите пример применения уголовных или административных норм в борьбе с разглашением защищаемой информации

8. Составьте перечень норм публичного права, направленных на борьбу с разглашением защищаемой информации.

9. Сравните зарубежный опыт борьбы с разглашением защищаемой информации с российским опытом.

Контрольные вопросы к практической работе №5 «Право собственности на информацию и интеллектуальнаясобственность»

1. Дайте определение понятию «интеллектуальная собственность».

2. Каково назначение интеллектуальной собственности?

3. Опишите состояние защиты интеллектуальной собственностив России в настоящее время.

4. Обоснуйте значение интеллектуальной собственности.

5. В чём заключается сущность интеллектуальной собственности?
6. Объясните, в чём разница между правом на информацию и правом на результаты интеллектуальной деятельности.
7. Каковы существенные особенности интеллектуальной собственности?
8. Приведите примеры объектов, содержащих интеллектуальную собственность.
9. Составьте перечень объектов, содержащих интеллектуальную собственность и информацию одновременно.
10. Сравните права на информацию с правами на результаты интеллектуальной деятельности.

Контрольные вопросы к практической работе №6 «Авторское право и лицензионные договоры»

1. Дайте определение понятию «авторское право».
2. Перечислите виды прав автора.
3. Дайте характеристику правам автора.
4. Обоснуйте необходимость правовой защиты прав автора.
5. В чём заключается сущность правовой защиты прав автора?
6. Оцените надёжность правовой защиты прав автора в России.
7. Объясните, в чём разница между авторским правом и правами автора.
8. Приведите примеры защиты прав автора.
9. Составьте перечень имущественных прав автора.
10. Сравните имущественные и личные неимущественные права автора.

Контрольные вопросы к практической работе №7 «Патентное право»

1. Дайте определение понятию «патентное право».
2. Перечислите виды патентных прав.
3. Дайте характеристику каждому имущественному и личному неимущественному праву патентообладателя.
4. Обоснуйте необходимость защиты патентных прав.
5. В чём заключается сущность патентного права?
6. Оцените надёжность защиты результатов интеллектуальной деятельности патентным правом.
7. Объясните, в чём разница между патентным и авторским правом.
8. Приведите примеры реализации патентных прав.
9. Составьте перечень имущественных прав изобретателя.
10. Сравните права автора произведения науки, литературы и искусства и права патентообладателя.

Контрольные вопросы к практической работе №8 «Правовой режим коммерческой тайны»

1. Каково назначение коммерческой тайны?
2. Чем вызвана необходимость защиты служебной тайны?
3. Оцените надёжность защиты при помощи права различных видов тайн.
4. Объясните, в чём разница между служебной и государственной тайной.
5. Каковы существенные особенности коммерческой тайны?
6. Приведите пример служебной тайны.
7. Сравните правовую защиту различных видов тайн в российском законодательстве.

Критерии оценки:

3 балла (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

2 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебныйматериал; иллюстрирует свой ответ типовыми примерами.

1 балл (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

0 баллов (или оценка «неудовлетворительно») выставляется обучающемуся, если он не владеет содержанием вопроса или допускает грубые ошибки; затрудняется дать основные определения; не может привести или приводит неправильные примеры; не отвечает на уточняющие и (или) дополнительные вопросы преподавателя или допускает при ответе на них грубые ошибки.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1.Меры информационной безопасности направлены на защиту от:

(1) нанесения неприемлемого ущерба

(2) нанесения любого ущерба

(3) подглядывания в замочную скважину

2. Меры информационной безопасности направлены на защиту от:

(1) нанесения неприемлемого ущерба

(2) нанесения любого ущерба

(3) подглядывания в замочную скважину

3.Что понимается под информационной безопасностью:
(1) защита душевного здоровья телезрителей

(2) защита от нанесения неприемлемого ущерба субъектам информационных отношений

(3) обеспечение информационной независимости России

4.Что из перечисленного не относится к числу основных аспектов информационной безопасности:
(1) доступность

(2) целостность

(3) конфиденциальность

(4) правдивое отражение действительности

5.Что из перечисленного не относится к числу основных аспектов информационной безопасности:
(1) доступность

(2) масштабируемость

(3) целостность

(4) конфиденциальность

6.Что из перечисленного не относится к числу основных аспектов информационной безопасности:
(1) доступность

(2) целостность

(3) защита от копирования

(4) конфиденциальность

7.Затраты организаций на информационную безопасность:
(1) растут

(2) остаются на одном уровне

(3) снижаются

8.Компьютерная преступность в мире:
(1) остается на одном уровне

(2) снижается

(3) растет

9.Средний ущерб от компьютерного преступления в США составляет примерно:
(1) сотни тысяч долларов

(2) десятки долларов

(3) копейки

10. Что из перечисленного относится к числу основных аспектов информационной безопасности:
(1) подлинность - аутентичность субъектов и объектов

(2) целостность - актуальность и непротиворечивость информации, защищенность информации и поддерживающей инфраструктуры от разрушения и несанкционированного изменения

(3) стерильность - отсутствие недекларированных возможностей

11. Что из перечисленного относится к числу основных аспектов информационной безопасности:
(1) подотчетность - полнота регистрационной информации о действиях субъектов

(2) приватность - сокрытие информации о личности пользователя

(3) конфиденциальность - защита от несанкционированного ознакомления

12. Сложность обеспечения информационной безопасности является следствием:
(1) комплексного характера данной проблемы, требующей для своего решения привлечения специалистов разного профиля

(2) наличия многочисленных высококвалифицированных злоумышленников

(3) развития глобальных сетей

13. Сложность обеспечения информационной безопасности является следствием:
(1) злого умысла разработчиков информационных систем

(2) объективных проблем современной технологии программирования

(3) происков западных спецслужб, встраивающих "закладки" в аппаратуру и программы

14. Сложность обеспечения информационной безопасности является следствием:
(1) невнимания широкой общественности к данной проблематике

(2) все большей зависимости общества от информационных систем

(3) быстрого прогресса информационных технологий, ведущего к постоянному изменению информационных систем и требований к ним

15. Как называется состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право?
(1) конфиденциальность

(2) доступность

(3) целостность

(4) аутентичность

16. Как называется состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право?
(1) конфиденциальность

(2) доступность

(3) целостность

(4) аутентичность

17. Как называется состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно?
(1) конфиденциальность

(2) доступность

(3) целостность

(4) аутентичность

18. Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?
(1) атака

(2) угроза

(3) уязвимость

(4) слабое место системы

19. Как называется попытка реализации угрозы?
(1) атака

(2) нападение

(3) уязвимость

(4) слабое место системы

20. Следствием наличия уязвимостей в информационной системе является:
(1) угроза

(2) атака

(3) нападение

(4) необходимость замены компонентов системы

21. Какой уровень защиты информации состоит из мер, реализуемых людьми?
(1) законодательный

(2) процедурный

(3) программно-технический

(4) административный

22. Какой уровень защиты информации представляет собой комплекс мер, применяемых руководством организации?
(1) законодательный

(2) процедурный

(3) программно-технический

(4) административный

23. На каком уровне защиты информации находятся непосредственно средства защиты?
(1) законодательный

(2) процедурный

(3) программно-технический

(4) административный

24. Совокупность содержащейся в базах данных информации, и информационных технологий и технических средств, обеспечивающих ее обработку, называется:
(1) система защиты информации

(2) автоматизированная система

(3) информационная система

(4) система обработки персональных данных

25. Как называется лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам?
(1) субъект персональных данных

(2) оператор информационной системы

(3) обладатель информации

(4) субъект информации

26. Как называется гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных?
(1) обладатель информации

(2) субъект информации

(3) обладатель информационной системы

(4) оператор информационной системы

27. Персональные данные это:
(1) любая информация, относящаяся к определенному, или определяемому на основании такой информации физическому лицу

(2) сведения (сообщения, данные) независимо от формы их представления

(3) любая информация, касающаяся физиологических особенностей человека

(4) информация, позволяющая связаться с человеком любым доступным способом

28. Как называется государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных?
(1) субъект персональных данных

(2) оператор информационной системы

(3) регулятор

(4) оператор персональных данных

29. Как называются органы, государственной власти, уполномоченные осуществлять мероприятия по контролю и надзору в отношении соблюдения требований ФЗ “О персональных данных”?
(1) операторы

(2) регуляторы

(3) контролеры

(4) надзорные органы

30. Какие категории персональных данных выделяет ФЗ “О персональных данных”?
(1) личные

(2) общедоступные

(3) физиологические

31. К какой категории персональных данных можно отнести адресную книгу?
(1) биометрические

(2) специальные

(3) дополнительные

(4) общедоступные

32. К какой категории персональных данных можно отнести сведения о национальной принадлежности человека?
(1) биометрические

(2) специальные

(3) дополнительные

(4) общедоступные

33. В каких случаях оператор не обязан уведомлять регулятора об обработке персональных данных?
(1) если данные включают в себя ФИО, телефон и размер оклада

(2) если оператора связывает с субъектом трудовые отношения

(3) если данные касаются здоровья субъекта

(4) если данные касаются семейной жизни субъекта

34. До начала обработки персональных данных оператор обязан:
(1) получить письменное согласие субъекта персональных данных
(2) получить устное согласие субъекта персональных данных
(3) уведомить регулятора о своем намерении в устной форме

35. Выберите случаи обработки персональных данных, когда оператор не обязан получать письменное согласие субъекта на обработку:
(1) бронирование гостиницы туристической фирмой

(2) передача данных третьим лицам

(3) организация составляет базу данных своих клиентов, с указанием ФИО, телефонов, адресов и занимаемых должностей

36. Обязанность по обеспечению безопасности персональных данных при их обработке полностью возлагается на:
(1) субъекта персональных данных

(2) оператора персональных данных

(3) доверенное лицо

(4) администратора безопасности информационной системы персональных данных

37. Если в результате несанкционированного доступа персональные данные были уничтожены, оператор обязан:
(1) уведомить об этом регулятора

(2) уведомить об этом субъекта персональных данных

(3) немедленно восстановить персональные данные

(4) произвести перенастройку средств защиты информации

38. Кто должен своевременно обнаруживать факты несанкционироанного доступа к персональным данным?
(1) оператор персональных данных

(2) субъект персональных данных

(3) регулятор

(4) контролер

39. Какой документ содержит в себе стратегические национальные приоритеты, цели и меры в области внутренней и внешней политики России, определяющие состояние национальной безопасности и уровень устойчивого развития государства на долгосрочную перспективу?
(1) Федеральный закон “Об информации, информационных технологиях и о защите информации”

(2) Федеральный закон “О государственной тайне”

(3) Доктрина информационной безопасности Российской Федерации

(4) Стратегия национальной безопасности Российской Федерации

40. Какие документы определяют общие отношение и политику государства в заданной области, а также служат основой для создания нормативно–правовых документов?
(1) концептуальные

(2) федеральные законы

(3) международные стандарты

(4) ГОСТЫ

41. Какой документ отображает официальные взгляды на цели, задачи, принципы и основные направления обеспечения информационной безопасности РФ?
(1) Федеральный закон “Об информации, информационных технологиях и о защите информации”

(2) Федеральный закон “О государственной тайне”

(3) Доктрина информационной безопасности Российской Федерации

(4) Стратегия национальной безопасности Российской Федерации

42. Кто такой инсайдер?
(1) сотрудник являющийся источником утечки информации

(2) любой источник утечки информации

(3) программа-вирус являющаяся источником утечки информации

43. Какая из ниже приведенных методик внедрения системы защиты против инсайдеров соответствует цели выявления канала утечки?
(1) открытое внедрение в сочетании с кадровой работой

(2) внедрение контролей, проверяемых при аудите

(3) скрытое внедрение в сочетании с ОРМ

(4) архивация движения данных и сетевых операций для доказательства того, что источник утечки не внутри фирмы

44. Какая из ниже приведенных методик внедрения системы защиты против инсайдеров соответствует цели соответствия требованиям нормативных актов и стандартов?
(1) открытое внедрение в сочетании с кадровой работой

(2) внедрение контролей, проверяемых при аудите

(3) скрытое внедрение в сочетании с ОРМ

(4) архивация движения данных и сетевых операций для доказательства того, что источник утечки не внутри фирмы

45. Кто должен доказывать виновность или невиновность сотрудника?
(1) работодатель

(2) сотрудник и его адвокат

(3) следственные органы

46. Для чего создается реестр конфиденциальных документов?
(1) для определения, какие документы являются конфиденциальными, какие сотрудники имеют доступ какого уровня к каким документам

(2) для классификации документов

(3) для выполнения требований законов

47. Анализ защищенности информационных систем проводится с помощью:
(1) межсетевых экранов

(2) сканеров безопасности

(3) браузеров

(4) команды ping

48. Электронные замки предназначены для:
(1) хранения большого объема конфиденциальной информации

(2) защиты периметра корпоративной сети

(3) надежной аутентификации и идентификации пользователей

(4) блокирования компьютера во время отсутствия пользователя на рабочем месте

49. Наличие межсетевого экрана необходимо при:
(1) использовании автономного автоматизированного рабочего места

(2) использовании изолированной локальной сети

(3) использовании сетей общего пользования

(4) использовании почтового ящика в сети Интернет

50."Информационная безопасность" - это:
(1) множество факторов, влияющих на состояние информационных ресурсов

(2) уровень защищенности информационных ресурсов

(3) совокупность методов управления информационными рисками

51.Информационная безопасность предполагает:
(1) нейтрализацию рисков

(2) повышение качества информационных ресурсов

52. Менеджмент в сфере информационной безопасности включает в себя:
(1) управление человеческими ресурсами

(2) решение криптографических задач

53. Разрушение информации является:
(1) сценарием нарушения информационной безопасности

(2) риском для информационных ресурсов

(3) угрозой информационной безопасности

54. Риски в сфере информационной безопасности разделяются на:
(1) внешние и внутренние

(2) объективные и субъективные

(3) системные и операционные

55..Международный союз электросвязи решает задачи:
(1) стандартизации протоколов безопасности

(2) финансирования фундаментальных научных исследований в сфере связи и безопасности

(3) содействия правоохранительным органам стран-членов союза при расследовании преступлений в сфере информационной безопасности

56. Членами ITU являются:
(1) независимые эксперты

(2) консультативные группы

(3) государственные органы

57. Сектором ITU, ответственным за стандартизацию технологий безопасности, является:
(1) ITU-R

(2) ITU-D

(3) ITU-T

58. Членство в ISO возможно для:
(1) государств

(2) частных компаний

(3) частных лиц

59. Членами ISO являются:
(1) университеты и компании, специализирующиеся на стандартизации

(2) независимые эксперты по стандартизации

(3) государственные органы по стандартизации

60.В организационную структуру ACM входят:
(1) группы специальных интересов

(2) комитеты по стандартам

(3) отраслевые департаменты

61.Задачи консорциума W3C включают в себя:
(1) стандартизацию подключения технических устройств к интернет

(2) стандартизация аппаратных средств защиты информации в интернет

62.Консорциум W3C занимается стандартизацией:
(1) технических устройств защиты информации

(2) программных средств защиты информации

(3) структур информации в интернете и подключения устройств к нему

63.Основным источником финансирования консорциума W3C является:
(1) отчисления за использование патентов

(2) членские взносы участников

(3) поступления из государственных фондов
64. Какой закон регулирует отношения, связанные с защитой детей от травмирующего их психику информационного воздействия, жестокости и насилия в общедоступных СМИ?
(1) "О защите персональных данных"

(2) "О защите детей от Интернета и СМИ"

(3) "О защите детей от информации, причиняющей вред их здоровью и развитию"

(4) "О защите интеллектуальных прав в Интернете"

65. Какой термин соответствует состоянию защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию?
(1) информационная целостность детей

(2) информационная защищенность детей

(3) информационная открытость детей

(4) информационная безопасность детей

66. Какой закон ввел обязанность владельцев интернет-сайтов удалить интернет-страницу, на которой размещается запрещенная к распространению информация, после получения соответствующего уведомления от хостинг-провайдера?
(1) ФЗ 64

(2) ФЗ 458

(3) ФЗ 139

(4) ФЗ 436

67. Какая ответственность предусмотрена за нарушение законодательства в области защиты детей от информации, причиняющей вред их здоровью и развитию?
(1) уголовная

(2) административная

(3) гражданская

68. Для кого административная ответственность за нарушение законодательства в области защиты детей от информации, причиняющей вред их здоровью и развитию, больше?
(1) для граждан

(2) для должностных лиц

(3) для предпринимателей

(4) для юридических лиц

69. Какой термин соответствует определению состояния защищенности личности, обеспечивающего ее целостность как активного социального субъекта и возможностей развития в условиях информационного взаимодействия с окружающей средой?
(1) информационная целостность личности

(2) информационная безопасность личности

(3) информационная защищенность личности

(4) информационная открытость личности

70. На каком сайте можно сообщить о неправомерном контенте?
(1) http://eais.rkn.gov.ru

(2) http://gov.ru

(3) http://reestr.ru

(4) http://eais.ru

71. В чем состоит основная цель создания реестра запрещенных сайтов? Выберите наиболее верное утверждение.
(1) ограничение доступа к сайтам, на которых нарушается авторское право

(2) ограничение доступа к сайтам, на которых размещается информация, запрещенная для распространения

(3) ограничение доступа к новостным сайтам

(4) наказание лиц, размещающих неправомерный контент на сайтах

72. Какой государственный орган ведет реестр запрещенных сайтов?
(1) ФСБ

(2) МВД

(3) Роскомнадзор

(4) Роскомстат

73. Какому уровню защиты детей от вредной информации соответствует создание "Стратегии национальной безопасности Российской Федерации до 2020 года"?

(1) концептуально-политический

(2) законодательный

(3) нормативно-технический

(4) административный

74. Какому уровню защиты детей от вредной информации соответствует создание ФЗ "О защите детей от информации, причиняющей вред их здоровью и развитию"?
(1) концептуально-политический

(2) законодательный

(3) нормативно-технический

(4) административный

75. Какому уровню защиты детей от вредной информации соответствует осуществление мероприятий по обеспечению безопасности в рамках конкретного предприятия?
(1) концептуально-политический

(2) законодательный

(3) нормативно-технический

(4) административный

76. Какому уровню защиты детей от вредной информации соответствует реализация идентификации, проверки подлинности, криптографии и аудита?
(1) программно-технический

(2) законодательный

(3) нормативно-технический

(4) административный

77. Какая категория мер по обеспечению ИБ подразумевает соблюдение школьниками норм и правил поведения в обществе при осуществлении информационной деятельности?
(1) правовое обеспечение информационной безопасности

(2) нравственный и этический контроль

(3) защита психики и здоровья ребенка

(4) организационная защита

78. К какой категории мер по обеспечению ИБ относится использование Родительского контроля?
(1) правовое обеспечение информационной безопасности

(2) нравственный и этический контроль

(3) защита психики и здоровья ребенка

(4) техническое и программное обеспечение ИБ

79. Какой принцип защиты детей от вредной информации предполагает формирование исчерпывающего комплекса мер по защите ребёнка от вредной информации и последовательную реализацию его во всех точках информационного пространства личности ребёнка?
(1) принцип объединения усилий всех заинтересованных сторон, при доминирующей позиции государства

(2) принцип непрерывности, последовательности и комплексности

(3) принцип построения системы защиты от вредоносной информации

(4) принцип открытости

80. Какой принцип защиты детей от вредной информации предполагает широкое информационное сопровождение деятельности по обеспечению информационной безопасности личности ребёнка?
(1) принцип объединения усилий всех заинтересованных сторон, при доминирующей позиции государства

(2) принцип непрерывности, последовательности и комплексности

(3) принцип построения системы защиты от вредоносной информации

(4) принцип открытости

81. К какой категории мер относится регламентация информационной деятельности подростков, контроль использования сетевых сервисов и сообществ, исключающие или ослабляющие нанесение вреда ЛИС школьника?

(1) правовое обеспечение информационной безопасности

(2) нравственный и этический контроль

(3) защита психики и здоровья ребенка

(4) организационная защита

82. Выделите верное утверждение в отношении информационной безопасности.
(1) наступление нового этапа развития ИТ приводит к быстрому повышению уровня информационной безопасности

(2) наступление нового этапа развития ИТ приводит к быстрому падению уровня информационной безопасности

(3) уровень информационной безопасности не зависит от этапов развития ИТ

83. Выделите верное утверждение в отношении информационной безопасности.
(1) технологии постоянно усложняются, однако квалификация нарушителей и злоумышленников понижается

(2) технологии постоянно усложняются, вместе с ними повышается квалификация нарушителей и злоумышленников

(3) технологии постоянно упрощаются, однако квалификация нарушителей и злоумышленников повышается

84. К какому уровню обеспечения ИБ относится «Доктрина информационной безопасности Российской Федерации»?
(1) законодательный

(2) административный

(3) процедурный

(4) научно-технический

85. К какому уровню обеспечения ИБ относятся действия общего и специального характера, предпринимаемые руководством организации?
(1) законодательный

(2) административный

(3) процедурный

(4) научно-технический

86. К какому уровню обеспечения ИБ относятся меры безопасности, закрепленные в соответствующих методологиях и реализуемые ответственными менеджерами и персоналом предприятия?
(1) законодательный

(2) административный

(3) процедурный

(4) научно-технический

87. К какому уровню обеспечения ИБ относятся конкретные методики, программно-аппаратные, технологические и технические меры?
(1) законодательный

(2) административный

(3) процедурный

(4) научно-технический

88. К какому уровню обеспечения ИБ относится «Политика информационной безопасности», утвержденная руководителем в конкретной организации?
(1) законодательный

(2) административный

(3) процедурный

(4) научно-технический

89. В организации проводятся проверки «чистый стол», целью которых является выявление нарушений требований по хранению ключевых носителей и конфиденциальных документов. К какому уровню обеспечения ИБ они относятся?
(1) законодательный

(2) административный

(3) процедурный

(4) научно-технический

90. Какой термин определяет защищенность жизненно важных интересов государственного или коммерческого предприятия от внутренних и внешних угроз, защиту кадрового и интеллектуального потенциала, технологий, данных и информации, капитала и прибыли, которая обеспечивается системой мер правового, экономического, организационного, информационного, инженерно-технического и социального характера?
(1) стратегическая безопасность

(2) информационная безопасность

(3) экономическая безопасность

(4) корпоративная безопасность

91. Какой термин определяет защищенность информации, ресурсов и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений — производителям, владельцам и пользователям информации и поддерживающей инфраструктуре?
(1) стратегическая безопасность

(2) информационная безопасность

(3) экономическая безопасность

(4) корпоративная безопасность

92. Какой аспект информационной безопасности отражает то, что защищенная информация должна быть доступна только тому, кому она предназначена?
(1) целостность

(2) конфиденциальность

(3) доступность

93. Какой аспект информационной безопасности отражает возможность за приемлемое время получить требуемую информационную услугу?
(1) целостность

(2) конфиденциальность

(3) доступность

94. Какой аспект информационной безопасности отражает актуальность и непротиворечивость информации, её защищенность от разрушения и несанкционированного изменения?
(1) целостность

(2) конфиденциальность

(3) доступность

95. Если злоумышленник прочитал передаваемое по сети Интернет сообщение, какое свойство информации он нарушил?
(1) целостность

(2) конфиденциальность

(3) доступность

96. Если злоумышленник подменил исходное сообщение, передаваемое по сети Интернет, какое свойство информации он нарушил?
(1) целостность

(2) конфиденциальность

(3) доступность

97. Если в результате DoS-атаки злоумышленников сайт перестал работать, какой аспект информационной безопасности был нарушен?
(1) целостность

(2) конфиденциальность

(3) доступность

98. Какой аспект ИБ наиболее актуален для провайдера Интернет-услуг?
(1) целостность

(2) конфиденциальность

(3) доступность

99. Какой аспект ИБ наиболее актуален для научно-исследовательских организаций, имеющих открытые Web-серверы?

(1) целостность

(2) конфиденциальность

(3) доступность

100. Какой аспект ИБ наиболее актуален для фармацевтической компании, занимающейся разработкой новых лекарств?

(1) целостность

(2) конфиденциальность

(3) доступность

Задания в открытой форме

1. … – это сфера деятельности, связанная с созданием, распространением, преобразованием и потреблением информации. Назовите субъекты информационных отношений.
2. … информации заключается в ее существовании в неискаженном виде, не измененном по отношению к некоторому ее исходному состоянию.
3. ... свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.
4. … свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.
5. Основные 7 принципов обеспечения информационной безопасности: …
6. Защита … – не разовое мероприятие, а непрерывный целенаправленный процесс, предполагаемый принятие соответствующих мер на всех этапах жизненного цикла защиты системы.
7. Важно правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми – это принцип …
8. на этапе разработки системы защиты в нее должна закладываться некая избыточность, которая позволила бы увеличить срок ее жизнеспособности – описывается принцип …
9. Определяются законодательными актами страны, которыми регламентируется правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил. Это … меры защиты информации.

10. Нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий. Это … меры защиты информации.

11. Представляют собой мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации. Это … меры защиты информации.

12. Реализуются в виде механических, электрических и электронных устройств, предназначенных для препятствования проникновению и доступу потенциального нарушителя к компонентам защиты. Это … меры защиты информации.

13. Представляют из себя программное обеспечение, предназначенное для выполнения функций защиты информации. Это … меры защиты информации.

14. … - это отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации.

15. … - это отношения, возникающие при создании и использовании информационных технологий и средств их обеспечения

16. … - это отношения, возникающие при защите информации и прав субъектов, участвующих в информационных процессах и информатизации

17. … - это отношения, возникающие

18. Документированная информация представляет собой обыкновенные данные, а подход, отождествляющий информацию и данные, носит название «...».

19. К сведениям … следует относить такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.

20. К … сведениям следует относить такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства или отраслям экономики РФ в одной или нескольких областях деятельности.

21. Понятие … тесно связано с понятием защиты информации и является реализацией системы защиты информации для конкретного объекта или одного из его структурных подразделений или конкретной работы.

Задания на установление соответствия

1. Установить соответствие

1) Целостность	а) заключается в ее существовании в неискаженном виде, не измененном по отношению к некоторому ее исходному состоянию.

2) Доступность	b) свойство, указывающее на необходимость введения ограничений на доступ к ней определенного круга пользователей.
3) Конфиденциальность	c) свойство, характеризующее способность обеспечивать своевременный и беспрепятственный доступ пользователей к интересующим их данным.

2. Установить соответствие

1) Системность целевая	a) Подразумевает единство организации всех работ по защите информации и их управления.
2) Системность пространственная	b) Защищенность информации рассматривается как составная часть общего понятия качества информации.
3) Системность временная	c) Защищенность основанная на принципе непрерывности функционирования системы защиты
4) Системность организационная	d) Защищенность рассматривается как увязка вопросов защиты информации

3. Установить соответствие

1) Принцип разумной достаточности	a) защита не должна обеспечиваться только за счет секретности структурной безопасности и алгоритмов функционирования ее подсистемы.
2) Принцип разумной избыточности	b) Должны быть реализованы принципы гибкости управления, обеспечивающие возможность настройки механизмов в процессе функционирования системы.
3) Принцип гибкости управления и применения	c) на этапе разработки системы защиты в нее должна закладываться некий потенциал, который позволил бы увеличить срок ее жизнеспособности.
4) Открытость алгоритмов и механизмов защиты	d) Необходимо правильно выбрать тот уровень защиты, при котором затраты, риск взлома и размер возможного ущерба были бы приемлемыми.

4. Установить соответствие

1) Первый фактор	a) прочность существующего механизма защиты, характеризующаяся степенью сопротивляемости этих механизмов попыткам их обхода или преодоления.
2) Второй фактор	b) величина ущерба, наносимого владельцу АСОД в случае успешного осуществления угроз безопасности
3) Третий фактор	c) каждый путь осуществления угрозы должен быть перекрыт соответствующим механизмом защиты

5. Установить соответствие мер защиты информации:

1) Правовые	a) Реализуются в виде механических, электрических и электронных устройств, предназначенных для препятствования проникновению и доступу потенциального нарушителя к компонентам защиты.
2) Морально-этические	b) Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации
3) Административные	c) К ним относятся нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий.
4) Технические	d) Определяются законодательными актами страны, которыми регламентируется правила использования, обработки и передачи информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

6. Установить соответствие мер защиты информации:

1) К сведениям особой важности следует относить	a) Все иные из числа сведений, составляющих государственную тайну.
2) К совершенно секретным сведениям	b) Такие сведения, распространение которых может нанести ущерб интересам министерства,

следует относить	ведомства или отраслям экономики РФ в одной или нескольких областях деятельности.
3) К секретным сведениям следует относить	c) Такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях деятельности.

7. Установить соответствие

1) Коммерческая тайна	a) Служебные сведения, которые не относятся к государственной тайне, доступ к которым ограничен органами государственной власти и федеральными органами исполнительной власти в соответствии с законодательством.
2) Служебная тайна	b) Режим конфиденциальности информации, позволяющий её обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду
3) Профессиональная тайна	c) Информация, полученная гражданами при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности.

8. Установить соответствие

1) Основные организационные и организационно-технические мероприятия по созданию и поддержанию функционирования системы защиты включают:	a) Мероприятия по обеспечению достаточного уровня физической защиты всех компонентов АСОД (противопожарная охрана, охрана помещений, пропускной режим, обеспечение сохранности и физической целостности средств вычислительной техники, носителей информации и т.п.).
2) Разовые мероприятия включают:	b) Распределение реквизитов разграничения доступа (пароли, ключи шифрования и т.д.).
3) Периодически проводимые мероприятия включают:	c) Общесистемные мероприятия по созданию научно-технических и методологических основ защиты АСОД.
4) Постоянно	d) Мероприятия проводимые и повторяемые

проводимые мероприятия включают:	только при полном пересмотре принятых решений.

9. Установить соответствие

1) Общедоступные персональные данные	a) Это персональные данные, касающиеся расовой или национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья.
2) Специальные категории персональных данных	b) Это персональные данные, доступ к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.
3) Биометрические персональные данные	c) Это сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность.

10. Между средствами и функциями

1) Человек, информация, технические средства	a) Информационное оружие
2) Целенаправленное производство и распространение специальной информации, оказывающей непосредственное влияние на функционирование и развитие психологической среды общества, психику и поведение населения, руководства страны, военнослужащих	b) Информационное воздействие
3) Комплекс технических средств и технологий, предназначенных для получения контроля над информационными ресурсами потенциального противника в целях выведения их из строя, получения или модификации содержащихся в них данных, целенаправленного продвижения выгодной информации (или дезинформации)	c) Элементы информационного пространства
4) Применение средств, позволяющих производить с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия	d) Психологическое воздействие

11. Установить соответствие:

1) Косвенные каналы	a) связанные с доступом к элементам АСОД, но не требующие изменения компонентов системы.
2) Прямые каналы	b) не связанные с физическим доступом к элементам АСОД.
3) Прямые каналы	c) связанные с доступом к элементам АСОД и изменением структуры компонентов АСОД.

12. Установить соответствие:

1) Нарушитель	a) намеренно идущий на нарушение из корыстных побуждений.
2) Злоумышленник	b) лицо, предпринявшее попытку выполнения запрещенных действий по ошибке, незнанию или осознанно со злым умыслом или без такового, и использующее для этого различные возможности, методы и средства.
3) взломщик	c) Лицо, которое с корыстными целями осуществляет несанкционированный доступ к данным или программам.

13. Установить соответствие нарушителей по уровням знания АСОД:

1) 1 уровень	a) Обладает высоким уровнем знаний и опытом работы с техническими средствами системы и ее обслуживания.
2) 2 уровень	b) Знает функциональные особенности АСОД, основные закономерности формирования в нестандартных массивах данных и потоков запросов к ним. Умеет пользоваться штатными средствами.
3) 3 уровень	4) Знает структуру, функции и механизмы действия средств защиты, их слабые и сильные стороны.
5) 4 уровень	6) Обладает уровнем знаний в области программирования и вычислительных технологий, проектирования и эксплуатации АСОД.

14. Установить соответствие нарушителей по времени действия:

1) 3 уровень	a) В период неактивности компонентов системы (нерабочее время, перерывы, ремонт и т.п.).
2) 2 уровень	b) Во время функционирования АСОД (во время работы компонентов системы).
3) 1 уровень	c) Как в процессе функционирования АСОД, так и в период неактивности системы.

15. Установить соответствие нарушителей по уровням возможностей (используемым методам и вопросам):

1) 1 уровень	a) Применяющие пассивные средства (технические средства перехвата без модификации компонентов системы).
2) 2 уровень	b) Применяющие только агентурные методы получения сведений
3) 3 уровень	c) Использующие только штатные средства и недостатки системы защиты, их сильные и слабые стороны.
4) 4 уровень	d) Применяющие методы и действия активного воздействия (модификация и подключение дополнительных технических устройств).

16. Установите соответствие

1) Геополитические проблемы	a) Технологии «мягкой силы» в геополитике Электронная слежка за политическими лидерами «Глобальное наблюдение» за населением Информационные и «гибридные» войны
2) Социальные проблемы	b) Информационная преступность Информационное неравенство. Манипуляции общественным сознанием. Виртуализация общества
3) Культурологические проблемы	c) Глобализация и культура Новая информационная культура общества Электронная культура Многоязычие в

	киберпространстве
4) Антропологические проблемы	d) Энергоинформационная безопасность Интеллектуальная безопасность Информационные факторы деструктивного поведения Информационные болезни Информационная видеоэкология

17. Установите соответствие между аспектами ИБ и их описанием

1) Личностно-социальный аспект	a) связан с проблемой социальной адаптации человека в новой, быстро изменяющейся информационной среде
2) Социально-экономический аспект	b) связан с национальной политикой той или иной страны в области развития информационной среды отдельных регионов и страны в целом, их информационной инфраструктуры, средств и методов доступа к информационным ресурсам и информационным коммуникациям
3) Геополитический аспект	c) связан с неравномерностью развития процесса информатизации в различных странах и регионах мира, что объясняется не только различиями в научно-техническом и экономическом потенциалах этих стран, но также и уровнем развития образования в этих странах, а также степенью понимания их политическими лидерами основных тенденций и закономерностей современного этапа развития цивилизации.

18.Установить соответствие между терминами и их значениями

1) Техническая сфера	a) область информационного пространства, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой функционируют системы управления, связи и разведки
2) Психологическая сфера	b) область информационного пространства, которая объединяет мышление личного состава ВС и мирного населения. Это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства, мораль, понятие сплоченности подразделений, уровень подготовки, опыт, понимание ситуации и общественное мнение

3) Информационная обстановка	c) совокупность людей, организаций и систем, собирающих, отрабатывающих, доводящих информацию или действующих на ее основе
4) Элементы информационной обстановки	d) руководители, лица, принимающие решения (ЛПР), люди организации и системы

19. Установить соответствие между типологиями «Информационных войн»

1) психологические операции	a) использование информации для воздействия b) на аргументацию солдат врага
2) электронная война	c) не позволяет врагу получить точную информацию
3) дезинформация	d) предоставляет врагу ложную информацию о наших силах и намерениях
4) физическое разрушение	e) может быть частью информационной войны, f) если имеет целью воздействие на элементы информационных систем

20. Установить соответствие между основными принципы защиты информации

1) Принцип законности	a) необходимо нормативно- правовое регулирование этой области общественных отношений. Законодательно должны быть обозначены права различных субъектов в области защиты информации
2) Принцип защиты информации	b) основополагающие идеи, важнейшие рекомендации по организации и осуществлению этой деятельности на различных этапах решения задач сохранения секретов
3) Принцип приоритета	c) объектом засекречивания не могут быть сведения, которые государство обнародует или сообщает согласно конвенциям или соглашениям
4) Принцип собственности и экономической целесообразности	d) право собственникам информации принимать меры к защите этой информации, а также оценивать ее потребительские свойства

Задания на установление правильной последовательности

1. Расположить современные проблемы информационного противоборства по их важности
1. По мере развития социальных институтов информационные процессы усложняются, что приводит к усложнению процессов принятия решения
2. Система — цель информационной войны может включать любой элемент в эпистемиологии противника
3. Буквально на наших глазах меняются технологии интернет-коммуникаций: если еще несколько лет назад основу составляли интернет-СМИ
4. Среди сетевых ресурсов все большую роль играют онлайновые социальные сети

2. Выделите по важности 3 части информационного противоборства
1.Стратегический анализ
2.Информационное воздействие
3.Информационное противодействие

3. Расположите по важности главные объекты информационно-психологического противоборства
1.психика политэлиты и населения противостоящих сторон
2.система формирования общественного сознания
3.система формирования общественно мнения
4.система принятия решений

4. Расположите по порядку основные формы информационного противоборства
1.информационное доминирование
2.информационная асимметрия
3.информационное сдерживание
4.информационная агрессия
5.контроль и управление информацией

5. Выберите правильную последовательность этапов развития информационной безопасности после первой половины 20-го века:
1.Обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.
2.Связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных

пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.

3. Связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

6. Выберите последовательность уровней защищенности персональных данных

1. специальные категории ПДн
2. биометрические ПДн
3. общедоступные ПДн
4. иные категории ПДн

7. Выберите правильную последовательность этапов защиты информации, информационных технологий и автоматизированных систем от атак:

1. Анализ рисков для активов организации, включающий в себя выявление ценных активов и оценку возможных последствий реализации атак с использованием скрытых каналов
2. Реализация защитных мер по противодействию скрытых каналов
3. Ор ганизация контроля за противодействием скрытых каналов.
4. Выявление скрытых каналов и оценка их опасности для активов организации

8. Выберите правильную последовательность этапов работы по обеспечению режима ИБ:

1. Выявление максимально полного множества потенциальных угроз, способов и каналов их осуществления;
2. Определение и выработка политики информационной безопасности;
3. Определение совокупности целей создания системы иб и сферы (границ) ее функционирования;
4. Выявление уязвимостей, проведение оценки рисков, формирование методик управление рисками;

9. Установите последовательность этапов работы по обеспечению информационной безопасности:

1. Определение требований к системе защиты информации;
2. Выбор контрмер, обеспечивающих режим иб, и средств защиты;
3. Разработка, внедрение и организация использования выбранных мер, способов и средств защиты;
4. Осуществление текущего контроля целостности информационных ресурсов и средств защиты и плановый аудит системы управления информационной безопасностью.

10. Выберите правильную последовательность этапов процесса управления рисками:

1. идентификация активов и ценности ресурсов, нуждающихся в защите;
2. анализ угроз и их последствий, определение слабостей в защите;
3. классификация рисков, выбор методологии оценки рисков и проведение оценки;
4. выбор, реализация и проверка защитных мер;
5. оценка остаточного риска;
6. выбор анализируемых объектов и степени детальности их рассмотрения;

11. Выберите правильную последовательность этапов развития информационной безопасности до первой половину 20-го века:

1. Характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.
2. Связан с началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне, а именно применение помехоустойчивого кодирования сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала).
3. Связан с появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.
4. Связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной

безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

12. Выберите правильную последовательность этапов развития информационной безопасности после первой половины 20-го века:

1. Обусловлен созданием и развитием локальных информационно-коммуникационных сетей. Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.
2. Связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьёзнее. Образовались сообщества людей — хакеров, ставящих своей целью нанесение ущерба информационной безопасности отдельных пользователей, организаций и целых стран. Информационный ресурс стал важнейшим ресурсом государства, а обеспечение его безопасности — важнейшей и обязательной составляющей национальной безопасности. Формируется информационное право — новая отрасль международной правовой системы.
3. Связан с созданием и развитием глобальных информационно-коммуникационных сетей с использованием космических средств обеспечения. Можно предположить что очередной этап развития информационной безопасности, будет связан с широким использованием сверхмобильных коммуникационных устройств с широким спектром задач и глобальным охватом в пространстве и времени, обеспечиваемым космическими информационно-коммуникационными системами. Для решения задач информационной безопасности на этом этапе необходимо создание макросистемы информационной безопасности человечества под эгидой ведущих международных форумов.

13. Выберите последовательность уровней защищенности персональных данных

1. специальные категории ПДн
2. биометрические ПДн
3. общедоступные ПДн
4. иные категории ПДн

14. Выберите последовательность уровней безопасности информации:

1. Административный уровень
2. Процедурный уровень
3. Программно-технический уровень

4. Законодательный уровень

15. Выберите последовательность проведения моделирования угроз:
1. Определение негативных последствий от угроз безопасности информации.
2. Определение объектов воздействия угроз безопасности информации.
3. Оценка возможности реализации угроз и их актуальности.

16. Выберите правильную последовательность этапов оценки угроз безопасности информации:
1. Определение негативных последствий, которые могут наступить от реализации (возникновения) угроз безопасности информации;
2. Инвентаризация систем и сетей и определение возможных объектов воздействия угроз безопасности информации;
3. Определение источников угроз безопасности информации и оценка возможностей нарушителей по реализации угроз безопасности информации;
4. Оценка способов реализации (возникновения) угроз безопасности информации;
5. Оценка возможности реализации (возникновения) угроз безопасности информации и определение актуальности угроз безопасности информации;
6. Оценка сценариев реализации угроз безопасности информации в системах и сетях.

17. Выберите правильную последовательность этапов построения политики безопасности:
1. Выбор и установка средств защиты;
2. Организация обслуживания по вопросам информационной безопасности;
3. Создание системы периодического контроля информационной безопасности
4. Обследование информационной системы на предмет установления организационной и информационной структуры и угроз безопасности информации;
5. Подготовка персонала работе со средствами защиты;

18. Выберите правильную последовательность этапов жизненного цикла информационного сервиса:
1. Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.
2. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

3. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.
4. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

19. Выберите правильную последовательность этапов построения системы защиты:
1. Анализ
2. Реализация системы защиты
3. Сопровождение системы защиты.
4. Разработка системы защиты

20. Выберите последовательность приоритетных этапов защиты информации:
1. Защита информации от несанкционированного доступа;
2. Защита информации в системах связи;
3. Защита юридической значимости электронных документов;
4. Защита конфиденциальной информации от утечки по каналам побочных электромагнитных излучений и наводок;
5. Защита информации от компьютерных вирусов и других опасных воздействий по каналам распространения программ;
6. Защита от несанкционированного копирования и распространения программ и ценной компьютерной информации.

Шкала оценивания результатов тестирования: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 баллов (установлено положением П 02.016).

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

Балл, полученный обучающимся за тестирование, суммируется с баллом, выставленным ему за решение компетентностно-ориентированной задачи.

Общий балл по промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно
49 и менее	неудовлетворительно

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1
Проанализировать современный уровень развития информационного оружия относительно развития и применения типов информационного оружия в конфликтах второй половины XX–начала XXI века

Компетентностно-ориентированная задача № 2
Рассмотреть компьютерную систему как объект информационного воздействия (с помощью информационного оружия). Описать методы нарушения конфиденциальности, целостности и доступности информации как угроз национальной безопасности.

Компетентностно-ориентированная задача № 3
На основе документов, определяющих политику государства в области национальной безопасности, следующих стран:
a. СтранЕвропейскогосоюза: «EU strategic communication to counteract anti-EU propaganda by third parties», «An Open, Safe and Secure Cyberspace».
b. США (The National Security Strategy).
определить следующее:
a. угрозы безопасности, существующие на уровне страны или нации (объекты и угрозы информационной войны);
b. источники угроз (внешние и внутренние);
c. национальные интересы (в том числе их основные составляющие) и угрозы информационной безопасности в информационной сфере;
d. основные направления обеспечения информационной безопасности государства, в том числе технических объектов информационной сферы государства в условиях информационной войны.

Компетентностно-ориентированная задача № 4
На основе документов, определяющих политику государства в области национальной безопасности, следующих стран:
a. СтранЕвропейскогосоюза: «EU strategic communication to counteract anti-EU propaganda by third parties», «An Open, Safe and Secure Cyberspace».
b. США (The National Security Strategy).

Произвести сравнение и анализ указанных выше документов между собой и с Доктриной информационной безопасности Российской Федерации. Выявить общие черты и отличия.

Компетентностно-ориентированная задача № 5

1. Провести сравнительный анализ опыта РФ и ведущих зарубежных стран в области противодействия информационно-психологическому воздействию.
2. На их основе пределить методы противодействия информационнопсихологическому воздействию (методы информационнопсихологического противодействия), методы защиты личности отинформационно-психологических воздействий в СМИ и СМК.

Компетентностно-ориентированная задача № 6

1. Приведите перечень средств информационно-психологического воздействия и манипулирования мнением и их описание (ложные авторитеты, сокрытие фактов, использование ярко выраженной эмоциональной окраски и пр.).
2. Отберите два информационных сообщения, размещенных в СМИ и/или СМК разными сторонами противоборства, на тему выбранного события.
3.Проведите фактологический анализ данных сообщений.

Компетентностно-ориентированная задача № 7

Выберите некоторое событие (информационный повод), вызвавшееактивные обсуждения, дискуссии в СМИ и СМК, по тематике которого велось активное информационное противоборство. Для события в целом определите заинтересованные стороны, цели, сценарии, используемые методы информационно-психологическоговоздействия.Отберите два информационных сообщения, размещенных в СМИи/или СМК разными сторонами противоборства, на тему выбранного события. Проведите фактологический анализ данных сообщений.

Компетентностно-ориентированная задача № 8

1. Провести сравнительный анализ опыта РФ и ведущих зарубежных стран в области противодействия информационно-психологическому воздействию.
2. На их основе сформулировать предложения по решению проблем, вызванныхнегативным влиянием информационных войн.

Компетентностно-ориентированная задача № 9

1. Определить характеристику канала коммуникации, СМИ/СМК и влияние их специфики на текст (направленность издания, интересы и потребности аудитории).
2. Дать характеристику текста с точки зрения его содержания: тема, замысел, идея как воплощение целевой установки.
3. Определить отношение автора к тематике сообщения.

4. Определить виды информации, использованной в тексте: описательная (фактологическая), оценочная (рефлексивная), нормативная, приведите обоснование.
5. Определить факторы, которые оказывают решающее влияния в организации фактического материала, выборе форм предъявления фактов и системы доказательств:
-назначение, функция, целевая установка текста – сообщить новость, рассказать о событии, явлении, проанализировать ситуацию, создать некоторый образ личности и прочие;
- объект отображения – область реальной действительности, которой касается сообщение или которую исследует автор статьи;
- предмет отображения и фактическая основа – факт (информационный повод «жесткая» или «мягкая» новость), ситуация, проблема, человек (а также факт, событие, явления, процессы, ситуации, сообщения СМИ, книги, фильмы – информационные явления, дающие повод для подготовки рецензий, обзоров).

Компетентностно-ориентированная задача № 10
1. Провести сравнительный анализ опыта РФ и ведущих зарубежных стран в области противодействия информационно-психологическому воздействию.
2. На их основе разработать предложения и рекомендации по совершенствованию действующей политики РФ и государственной политики в информационнойсфере с учетом международного опыта.

Шкала оценивания решения компетентностно-ориентированной задачи: в соответствии с действующей в университете балльно-рейтинговой системой оценивание результатов промежуточной аттестации обучающихся осуществляется в рамках 100-балльной шкалы, при этом максимальный балл по промежуточной аттестации обучающихся по очной форме обучения составляет 36 баллов, по очно-заочной и заочной формам обучения – 60 (установлено положением П 02.016).

Максимальное количество баллов за решение компетентностно-ориентированной задачи – 6 баллов.

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

Сумма баллов по 100-балльной шкале	Оценка по 5-балльной шкале
100-85	отлично
84-70	хорошо
69-50	удовлетворительно

49 и менее	неудовлетворительно

Критерии оценивания решения компетентностно-ориентированной задачи (нижеследующие критерии оценки являются примерными и могут корректироваться):

6-5 баллов выставляется обучающемуся, если решение задачи демонстрирует глубокое понимание обучающимся предложенной проблемы и разностороннее ее рассмотрение; свободно конструируемая работа представляет собой логичное, ясное и при этом краткое, точное описание хода решения задачи (последовательности (или выполнения) необходимых трудовых действий) и формулировку доказанного, правильного вывода (ответа); при этом обучающимся предложено несколько вариантов решения или оригинальное, нестандартное решение (или наиболее эффективное, или наиболее рациональное, или оптимальное, или единственно правильное решение); задача решена в установленное преподавателем время или с опережением времени.

4-3 балла выставляется обучающемуся, если решение задачи демонстрирует понимание обучающимся предложенной проблемы; задача решена типовым способом в установленное преподавателем время; имеют место общие фразы и (или) несущественные недочеты в описании хода решения и (или) вывода (ответа).

2-1 балла выставляется обучающемуся, если решение задачи демонстрирует поверхностное понимание обучающимся предложенной проблемы; осуществлена попытка шаблонного решения задачи, но при ее решении допущены ошибки и (или) превышено установленное преподавателем время.

0 баллов выставляется обучающемуся, если решение задачи демонстрирует непонимание обучающимся предложенной проблемы, и (или) значительное место занимают общие фразы и голословные рассуждения, и (или) задача не решена.