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
История информационного противоборства
(наименование дисциплины)

10.03.01Информационная 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. История возникновения органов защиты информации.

1. Криптография в древнем мире.
2. История появления первых служб информационного противодействия.
3. Первые законодательные акты в области информационной безопасности.
4. Появление понятия «государственная тайна».
5. Влияние развития средств коммуникации на деятельность по обеспечению информационной безопасности
6. Какие исторические факторы способствовали появлению первых органов по защите информации?
7. Какие первоначальные методы и техники использовались для защиты информации в древности?
8. Какие органы были первыми в мире, занимавшимися защитой информации, и в каких странах они возникли?
9. Какие изменения в социуме привели к появлению специализированных органов по защите информации?
10. Какова роль революций и технологического прогресса в развитии органов защиты информации?

Тема 2. Защита государственных интересов в XII – XVI вв.

1. Влияние информационной разведки на успешность средневековых боевых операций.
2. Особенности политического устройства России в12-16 вв., влияющие на обеспечение защиты государственных интересов
3. Особенности защищённой переписки в средние века
4. Правовое регулирование защиты государственных интересов.
5. Какие методы и средства использовались для обеспечения безопасности государства в средние века?
6. Каким образом величие и мощь государства влияли на меры по защите его интересов?
7. Какие роли играли шпионы и контрразведка в этот период?
8. Как влияли войны и торговля на уровень безопасности государственных интересов?
9. Каким образом смена династий и властителей влияла на стратегии защиты государства?
10. Какие изменения в социуме в данный период времени привели к появлению специализированных органов по защите информации?

Тема 3. Защита государственных интересов в XVI - XVIII вв.

1. Внешняя разведка Российского государства в период 16-18 вв.
2. Органы государственной безопасности Российского государства в период 16-18 вв .
3. Аналитическая работа внешней разведки Российского государства в период 16-18 вв
4. Особенности региональной политики в области защиты государственных интересов
5. Как развивалась система информационной разведки и контрразведки в период Ренессанса и Просвещения?
6. Какие новые подходы к защите государственных интересов появились в период Колумбовых открытий и эпохи Великих географических открытий?
7. Какие роли играли дипломатия и шпионаж в защите государственных интересов в указанный период?
8. Как влияли войны религиозных конфессий на меры по защите государственной безопасности?
9. Какие тенденции в развитии научно-технического прогресса оказывали влияние на методы защиты государственных интересов?
10. Какие изменения в социуме в данный период времени привели к появлению специализированных органов по защите информации?

Тема 4. Защита государственных интересов в XIX веке.

1. Органы, отвечающие за обеспечение информационной безопасности в Российской Империи
2. Борьба со шпионажем в 18 в.
3. Используемы методики агентурной разведки и ОРМ
4. Розыск преступников в 19 в.
5. Правила защищённого документооборота в 19 в.
6. Ответственность должностных лиц за нарушение режима защищённого документооборота
7. Какие главные угрозы и вызовы стояли перед государствами в XIX веке, требующие эффективных мер по защите государственных интересов?
8. Какие новые технологии и методы коммуникации в XIX веке повлияли на развитие средств защиты информации и государственной безопасности?
9. Какие роли играли армии и дипломатия в обеспечении защиты государственных интересов в это время?
10. Как влияли национальные революции и войны на меры по обеспечению безопасности государства в XIX веке?

Тема 5. Защита государственных интересов в 1900-1917 гг.

1. Органы политического сыска.
2. Военная разведка в начале 20 в.

3. Основные достоинства разведки и контрразведки Российской империи
4. Какие ключевые события и изменения в мире сказались на стратегиях защиты государственных интересов в данный период времени?
5. Какие изменения в социуме в данный период времени привели к появлению специализированных органов по защите информации?
6. Какие вызовы и процессы в мировом сообществе повлияли на потребность в усилении защиты государственных интересов в начале XX века?
7. Какие реформы и новации были внедрены для усиления государственной безопасности в период 1900-1917 гг.?
8. В чем заключались главные угрозы для государств в начале XX века, требующие разработки новых стратегий защиты?
9. Как влияли революции, технологический прогресс и международные конфликты на методы защиты государственных интересов в этот период?
10. Каковы были основные тенденции в развитии геополитики и как они повлияли на стратегии безопасности государств?

Тема 6. Защита государственных интересов в период создания Советской власти и НЭПа.

1. Функции ВЧК.
2. Законодательные акты Советской власти в области информационного противоборства.
3. Функции Военно-статистического отдела
4. Назначение специального института консультантов при начальнике Региструпра
5. Структура и функции ГПУ
6. Особенности структур, отвечающих за информационное противоборство
7. Какие угрозы и вызовы стояли перед Советской властью в период создания и утверждения своей власти, требуя усиления мер по защите государственных интересов?
8. Какие новые подходы к организации безопасности применялись в период формирования Советской России и НЭПа?
9. Каким образом была организована контрразведка и спецслужбы для обеспечения безопасности государства в этот период?
10. Как важные события и реформы в идеологической и политической сфера влияли на стратегии защиты государственных интересов?

Тема 7. Защита государственных интересов в 1928 – 1941 годах.

1. Изменение структуры военной разведки
2. Борьба с иностранными агентами
3. Возникновение советской резедентурной сети.
4. Промышленный шпионаж со стороны СССР

5. Какие основные угрозы и вызовы стояли перед Советским государством в период индустриализации и коллективизации, требуя усиленной защиты государственных интересов?
6. Каким образом развивались структуры контрразведки, спецслужб и армии в период смены вождей и становления тоталитарного режима?
7. Как важные события, как Великая депрессия и международные конфликты, влияли на стратегии защиты государственных интересов?
8. Какие реформы и инновации были внедрены для усиления безопасности государства в период советской индустриализации?
9. Какие ключевые моменты во внешней и внутренней политике повлияли на развитие системы безопасности и контрразведку в 1928-1941 годах?
10. Какие изменения внутри страны и на международной арене в этот период сказались на системе безопасности и защите информации?

Тема 8. Защита государственных интересов в период великой отечественной войны.

1. Структура органов госбезопасности.
2. Основные успешные операции органов госбезопасности.
3. Методы пропаганды, используемые во время ВМВ.
4. Какие наиболее значительные угрозы и вызовы стояли перед Советским государством в период Великой Отечественной войны, требуя жестких мер по защите государственных интересов?
5. Как величие войны повлияло на организацию государственной безопасности и специализированных органов военного контрразведывательного ведомства?
6. Каким образом развивались спецслужбы и контрразведка в условиях военного времени, включая противодействие шпионам и диверсантам?
7. Какие новые технологии и методы защиты информации использовались в условиях войны и оккупации?
8. Какие уроки и изменения были внесены в систему безопасности государства после окончания Великой Отечественной войны?
9. Какие тенденции в развитии научно-технического прогресса оказывали влияние на методы защиты государственных интересов?
10. Какие изменения в социуме в данный период времени привели к появлению специализированных органов по защите информации?

Тема 9. Система безопасности СССР и России в XX – XXI веках

1. Функции структур, отвечающих за информационное противодействие
2. Работа с пропагандистскими инструментами
3. Информационные войны в современном мире
4. Средства ведения информационных войн.
5. Технологии манипулирования общественным мнением

6. Каковы основные принципы и структуры системы безопасности в СССР и, позднее, в современной России, и как они эволюционировали со временем?
7. Как важные события, как распад Советского Союза и террористические угрозы, повлияли на модернизацию системы безопасности?
8. Каким образом развивались спецслужбы, контрразведка, и вооруженные силы в XXI веке для обеспечения национальной безопасности?
9. Какие изменения в технологиях и методах шпионажа и терроризма предъявляют новые требования к системе безопасности?
10. Какие вызовы и угрозы современности накладывают свой отпечаток на стратегии защиты государственных интересов в Росии XXI века?

Критерии оценки:

10-12 баллов (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.

7-9 баллов (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.

1-6 баллов (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

Практическая работа № 1 «Информационная безопасность в системе национальной безопасности государства»

1. Каково значение информационной безопасности для обеспечения национальной безопасности государства?
2. Какие угрозы представляют собой кибератаки и кибершпионаж для информационной безопасности государства?
3. Какие методы и технологии используются для защиты государственной информации от киберугроз?
4. Каким образом информационные войны могут повлиять на стабильность и безопасность государства?
5. Как влияют социальные сети и интернет-платформы на информационную безопасность государства?
6. Какие стратегии и политики разрабатываются для защиты информационной безопасности национального уровня?
7. Как стимулируется сотрудничество между государствами в борьбе за информационную безопасность?
8. Какие организации и структуры ответственны за обеспечение информационной безопасности на уровне государства?
9. Какие законы и нормативные акты регулируют информационную безопасность национального уровня?
10. Какие вызовы предстоят в области информационной безопасности в будущем?

Практическая работа № 2 «Методы и средства информационного противоборства и информационно-психологического воздействия в современных СМИ и СМК»

1. Какие методы информационного противоборства используются в современных средствах массовой информации (СМИ)?
2. В чем заключается информационно-психологическое воздействие и каковы его цели при использовании в СМИ и социальных медиа?
3. Как влияют методы манипуляции информацией на общественное мнение и политические процессы через СМИ?
4. Каким образом современные редакции и журналисты могут бороться против информационного противоборства и фейковых новостей?
5. Какие технологии и инструменты используются для анализа информационного противоборства и фильтрации ложной информации?
6. Какова роль социальных сетей и онлайн-платформ в распространении информационно-психологического воздействия?
7. Какие законы и правила регулируют деятельность информационных агентств и СМИ с целью предотвращения информационного противоборства?

8. Как различные политические группы и государства могут использовать информационно-психологическое воздействие для достижения своих целей?

9. Как можно различить нейтральные и объективные информационные сообщения от пропагандистских и манипулятивных?

10. Каковы последствия использования информационно-психологического воздействия через СМИ для общества и политической среды?

Практическая работа № 3 «Фактологический анализ информационных сообщений для выявления применения методов информационно-психологического воздействия»

1. Как проводится анализ информационных сообщений для выявления манипуляций и информационно-психологического воздействия?

2. Какие признаки и индикаторы указывают на возможное использование методов информационно-психологического воздействия в информационных материалах?

3. Каковы основные стратегии и методы выявления фейковых новостей и ложной информации в новостных потоках?

4. Как современные технологии и алгоритмы помогают автоматизировать фактологический анализ информации для выявления манипуляций?

5. Как можно оценить негативное воздействие манипулятивных новостей на общественное мнение и психологию граждан?

6. Какие методы и подходы используются для контроля за качеством информационных материалов и их соответствию фактам?

7. Как сотрудничество между информационными аналитиками и специалистами по психологии помогает в борьбе с информационным противоборством?

8. Каким образом инструменты цифровой аналитики могут быть использованы для выявления манипуляций и массового информационного воздействия?

9. Как важно обучение и информационная грамотность граждан для предотвращения распространения ложной информации и манипуляций?

10. Какие вызовы и проблемы стоят перед специалистами при осуществлении фактологического анализа с целью предотвращения информационного противоборства?

Критерии оценки:

7-8 баллов (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.

5-6 баллов (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.

1-4 балла (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.

1.3 КЕЙС-ЗАДАЧИ

Кейс №1: Криптография во время Холодной войны

Ситуация для обсуждения: В период Холодной войны криптография играла важную роль в информационном противоборстве между СССР и США. Обе стороны активно использовали шифровальные системы, чтобы защищать секретные сообщения и разгадывать коды противника.

Задание: Студентам предлагается изучить следующие аспекты:

- Ключевые шифровальные системы, использованные в период Холодной войны.
- Результаты успешного дешифрования кодов противника.
- Влияние криптографии на развитие событий и принятие политических решений.

Вопросы для обсуждения:

1. Какое значение имела Ультра и дешифровка энигмы в ходе Второй мировой войны и послевоенного периода?
2. Каким образом использование новых криптографических технологий влияло на преимущество в информационном противоборстве?
3. Какие проблемы шифрования и дешифрования сообщений могли возникнуть на фоне Холодной войны?
4. В какой мере современные методы криптографии отличаются от примененных в период Холодной войны?

Кейс №2: Разведывательная деятельность во время Второй мировой войны

Ситуация для обсуждения: Во время Второй мировой войны разведывательная деятельность имела ключевое значение для обеих сторон конфликта. Разведывательные службы собирали разнообразную информацию о планах противника, его вооружении, перемещениях войск и стратегических целях. Они использовали шпионов, радиосвязь, кодовые сообщения и другие методы для передачи и получения информации.

Задание: Студентам предлагается провести исследование по следующим пунктам:

- Операции разведывательных служб основных участников войны (например, SIS, Особый отдел НКВД, OSS).
- Методы сбора информации, используемые шпионами и разведчиками.
- Роль разведывательных отчетов в принятии стратегических решений.

Вопросы для обсуждения:

1. Каким образом разведывательная деятельность влияла на исход ключевых боевых операций во время Второй мировой войны?
2. Как использование кодированных сообщений и шифров способствовало сохранению конфиденциальности информации во время войны?
3. В чем состояли основные слабые места и ошибки в разведывательной работе сторон конфликта?
4. Какое воздействие имели дешифрованные сообщения противника на тактические и стратегические решения главнокомандующих?

Кейс №3: Кибератаки в современных конфликтах

Ситуация для обсуждения: В наше время кибератаки стали важным инструментом информационного противоборства как между странами, так и между корпорациями. Хакеры могут атаковать информационные системы, причиняя серьезный ущерб для враждующих сторон.

Задание: Студентам предлагается исследовать следующие аспекты:

- Типы кибератак, используемые в современных конфликтах.
- Меры защиты от киберугроз и противодействие хакерским атакам.
- Последствия успешных кибератак на государственные и коммерческие организации.

Вопросы для обсуждения:

1. Какие стратегии кибератак широко используются в современных конфликтах, и каковы их цели?
2. Как регулярное обновление информационных систем влияет на их устойчивость к кибератакам?
3. В чем состоит роль государства и международных организаций в предотвращении и реагировании на киберугрозы?
4. Каким образом кибератаки могут повлиять на гражданское население и общественные институты?

Критерии оценки:

10-12 баллов (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.

7-9 баллов (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.

1-6 баллов (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. В каком году была основана английская разведывательная служба MI6?
    - A) 1909
    - B) 1910
    - C) 1905
    - D) 1922
2. Каким методом использовались шифры во время античных войн?
    - A) Скоранный метод
    - B) Ксероксный метод
    - C) Цезарьский шифр
    - D) Иероглифический метод
3. Как называлась операция американской разведывательной службы во время Второй мировой войны, направленная на перехват кодированных сообщений?
    - A) Proyect Phoenix
    - B) Operation Overlord
    - C) Operation Venona
    - D) Task Force Alpha
4. Когда было создано КГБ как главное советское разведывательное агентство?
    - A) 1950
    - B) 1954
    - C) 1922
    - D) 1946
5. Кто был известен как "отец современной криптографии"?
    - A) Алан Тьюринг
    - B) Энигма
    - C) Ричард Фейнман
    - D) Джулия Ловлейс
6. Какую роль сыграло расшифровывание немецкого кода Енигма в ходе Второй мировой войны?
    - A) Помогло сохранить конфиденциальность секретных разработок Гитлера
    - B) Позволило английским и американским разведчикам получить доступ к секретной информации
    - C) Не имело существенного влияния на ход войны
    - D) Стало причиной поражений союзников

7. Какая страна разработала первый компьютер ENIAC, который использовался для криптоанализа немецких кодов во время Второй мировой войны?
    - A) США
    - B) Великобритания
    - C) СССР
    - D) Германия
8. Каким образом шифровальная машина Lorenz отличалась от шифровальной машины Енигма?
    - A) Lorenz использовала механические ключи, а Енигма - электрические
    - B) Lorenz была разработана в США, а Енигма - в Германии
    - C) Lorenz использовалась для шифрования военных сообщений, а Енигма - для цивильных
    - D) Lorenz проще в использовании, чем Енигма
9. В каком году был основан Центральный разведывательный управления США (CIA)?
    - A) 1947
    - B) 1950
    - C) 1960
    - D) 1945
10. Что означает аббревиатура OSS, связанная с историей информационного противоборства?

- A) Office of Secret Strategies
- B) Office of Strategic Services
- C) Office of Special Secrets
- D) Office of Secure Systems

11. Как называлась группа, осуществлявшая дешифрование сообщений немецких подводных лодок во время Второй мировой войны?

- A) Ultra
- B) Enigma Codebreakers
- C) Operation Barbarossa
- D) U-Boot Decryptors

12. В каком году была разгадана немецкая кодовая машина Енигма?

- A) 1943
- B) 1944
- C) 1941
- D) 1945

13. Какую роль сыграла разведка в ходе Карибского кризиса?

- A) Сообщила о подготовке Кубой ядерных ракет
- B) Помогла президенту США принять решение о начале военной операции
- C) Не играла решающей роли в решении конфликта
- D) Передала фальшивую информацию о противнике

14. Какой метод шифрования используется для защиты информации в сети Интернет?
- A) RSA
- B) Линейный блочный криптосистемный метод
- C) Азбучный метод
- D) Перестановочный метод

15. Как называется алгоритм шифрования, который используется для обеспечения безопасной передачи данных в Интернете?
- A) AES
- B) HTML
- C) SQL
- D) PHP

16. Каким образом Edward Snowden раскрыл информацию о программе массового слежения граждан США американскими разведывательными службами?
- A) Публично опубликовал документы в интернете
- B) Передал документы журналистам
- C) Скопировал данные на внешний носитель и унес из офиса
- D) Рассказал своему другу, который заявил властям

17. Как называется специальное программное обеспечение, которое позволяет хакерам получить доступ к компьютерной системе путем обхода стандартных мер защиты?
- A) Вирус
- B) Спам
- C) Троян
- D) Фишинг

18. Какую роль сыграла информационная война в ходе конфликта между Россией и Украиной?
- A) Помогла управлять общественным мнением
- B) Не оказала влияния на ход событий
- C) Была причиной эскалации конфликта
- D) Стала причиной массовых протестов

19. Какая страна является лидером по созданию и использованию кибероружия?
- A) США
- B) Китай
- C) Россия
- D) Израиль

20. Каким образом кибератаки влияют на демократические процессы в различных странах?
    - A) Усиливают доверие граждан к правительству
    - B) Могут оказать влияние на результаты выборов
    - C) Не влияют на работу демократии
    - D) Приводят к восстановлению правового порядка

21. Как называется вирус, известный своим воздействием на иранскую ядерную программу?
    - A) Stuxnet
    - B) WannaCry
    - C) Zeus
    - D) Conficker
22. Какую информацию предоставляет разведывательный отчет?
    - A) Анализ материалов маркетинговых исследований
    - B) Сведения о противнике, полученные разведывательными службами
    - C) Статистические данные о демографии
    - D) Информацию о политических лидерах
23. Как называется метод перехвата радиосигналов для получения секретной информации?
    - A) RADAR
    - B) SONAR
    - C) SIGINT
    - D) LIDAR
24. Каким образом шпионы могут использовать технику стеганографии для передачи секретной информации?
    - A) Встраивают сообщения в изображения или звуки
    - B) Шифруют информацию с помощью специальных алгоритмов
    - C) Передают сообщения через физическое лицо-носителя
    - D) Размещают информацию на открытых интернет-ресурсах
25. Какое из следующих утверждений является верным относительно роли разведывательной деятельности в течение истории?
    - A) Разведка влияла только на военные конфликты
    - B) Разведка играла ключевую роль в политических событиях
    - C) Разведка не имела важности до развития интернета
    - D) Разведка не влияла на развитие науки и технологий
26. Какие действия могут быть классифицированы как кибератаки?
    - A) Защита от взлома компьютерных систем
    - B) Отправка спам-писем
    - C) Удаление вирусов с компьютеров
    - D) Навязывание ресурсам большой нагрузки для отказа в обслуживании
27. Как можно защитить информацию на компьютере от кибератак?
    - A) Регулярно обновлять антивирусное ПО
    - B) Использовать сложные пароли и шифрование
    - C) Скачивать файлы из ненадежных источников
    - D) Публично делиться личной информацией в сети
28. Какова роль международных организаций, таких как ООН, в предотвращении киберугроз?
    - A) Разработка законодательства по кибербезопасности
    - B) Хакерские атаки на организации

- C) Проведение кибератак на другие страны
- D) Использование криптовалют для финансирования терроризма

29. Как кибератаки могут быть использованы в информационной войне между странами?
    - A) Для мирных целей без намерения причинить вред
    - B) Для вмешательства во внутренние дела другой страны
    - C) Для укрепления дружественных отношений с соседями
    - D) Для повышения качества образования через доступ к онлайн-ресурсам
30. Каким образом кибератаки могут повлиять на гражданское население в стране?
    - A) Повышение уровня киберграмотности и безопасности
    - B) Угроза национальной безопасности и доверия к правительству
    - C) Улучшение уровня занятости и экономического роста
    - D) Повышение уровня защищенности государственных информационных систем
31. Какие методы использовали американские и советские разведывательные службы для сбора информации во время Холодной войны?
    - A) Шпионы и допросы заключенных
    - B) Телескопы и спутники
    - C) Дроны и беспилотные летательные аппараты
    - D) Сверхзвуковые самолеты и подводные лодки
32. Какая роль отведена шифровальным методам в информационном противоборстве?
    - A) Защита конфиденциальной информации и разделение доступа
    - B) Публичная декларация стратегических целей
    - C) Расшифровка сообщений противника за счет разведывательных служб
    - D) Нанесение ущерба инфраструктуре стран-противников
33. Как современные технологии влияют на технику сбора разведывательной информации?
    - A) Увеличение скорости и точности сбора данных
    - B) Снижение качества информации и ее достоверности
    - C) Ограничение сферы применения разведывательной деятельности
    - D) Увеличение количества ошибок и искажений в отчетах разведчиков
34. Какие последствия могут иметь ошибки разведывательных служб на исход конфликта?
    - A) Увеличение шансов на победу и ослабление стратегии противника
    - B) Потеря доверия союзников и опасность для национальной безопасности

- C) Повышение уровня секретности и обеспечение конфиденциальности данных
- D) Укрепление позиций дипломатических отношений и урегулирование конфликта

35. Какова роль криптографии в современном информационном противоборстве?
    - A) Защита информации от несанкционированного доступа
    - B) Создание совравенных систем массовой слежки
    - C) Поддержание прозрачности и открытости правительства
    - D) Ограничение свободы слова и информационных потоков
36. Какие методы криптографии считаются наиболее надежными для защиты данных в сети?
    - A) Стеганография
    - B) Квантовая криптография
    - C) Шифрование симметричных ключей
    - D) Общественные ключи и алгоритм RSA
37. Какое понятие описывает использование фальшивой информации для манипуляции общественным мнением?

A) Дезинформация
B) Кибершпионаж
C) Штурм мозгов
D) Кибертерроризм

38. Какие методы могут быть использованы для проверки достоверности информации в цифровой эпохе?

A) Фактчекинг и анализ источников
B) Цензура и блокировка непроверенных источников
C) Агрессивное распространение лжи и мифов
D) Изгнание недоверенных журналистов и блогеров

39. Какие меры могут быть предприняты для защиты информации и борьбы с информационным противоборством?

A) Обучение общества критическому мышлению и цифровой грамотности
B) Усиление цензуры и государственное контролирование СМИ
C) Изоляция страны от глобальной сети Интернет
D) Активное использование дезинформации для контроля над общественным мнением

40. Основной критерий содержания эффективной пропаганды:

А) Наличие центрального тезиса.
Б) Лёгкость для понимания целевой аудиторией.
В) Сложность для критики.
Г) Привлекательность фона.

Задания в открытой форме

1. Основными объектами _____ воздействия являются, с одной стороны, _____-_____ системы различного масштаба и назначения, с другой - организационно-психологические объекты (психика отдельной личности; психологические явления и процессы в социальных общностях, группах различного масштаба, в обществе в целом; феномены общественного сознания; социальнополитические системы и процессы).
2. Исходя из этого, выделяются два основных направления _____-_____— информационно-техническое (ИТ) и информационно-психологическое (ИП).
3. Основой _____-_____борьбы являются средства массовой информации и коммуникации.
4. _____ _____ — это соперничество социальных систем в информационно-психологической сфере с целью усиления влияния на определенные сферы социальных отношений и установления контроля над источниками стратегических ресурсов.
5. _____ информационного противоборства является любой объект, в отношении которого возможно осуществление информационного воздействия (в том числе — применение информационного оружия) либо иного воздействия (силового, политического, экономического и т.д.), результатом которого будет модификация его свойств как информационной системы.
6. Объектом информационного противоборства может стать любой компонент или сегмент информационно-психологического пространства, в том числе — следующие виды: _____.
7. К субъектам информационного противоборства относят _____.
8. Проблемы в области безопасности электронного бизнеса включают_____.
9. Основные функциональные компоненты организации комплексной системы информационной безопасности_____.
10. _____— ставит перед собой цель лишить контроля налаженную связь между командованием и исполнителем.
11. _____ _____ — предусматривает сбор ценной информации для нападения и собственной защиты. Электронная война — целью является вывод из строя всех электронных коммуникаций.
12. _____ _____ — взлом и доступ к любым данным (электронная почта, банковские карты, личные файлы, переписки и так далее) и несанкционированное их использование. Экономическая война — информационная блокада (ограничение

коммерческой деятельности) или информационный империализм (политическая информационная атака).

13. _____ _____ — ставит перед собой цель захватить компьютерные данные, выследить объект, нарушить работу инфраструктуры, полагающейся на информационные технологии.
14. Электронная война направлена против средств электронных коммуникаций_____.
15. Психологическая война - пропаганда, информационная обработка населения, направленная на_____.
16. Хакерская война подразумевает диверсионные действия против_____.
17. Кибервойна отличается от "обычного" хакерства_____.
18. К служебной тайне не относится _____
19. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений которые_____
20. Не представляют угрозу информационной безопасности общества_____

Задания на установление соответствия

1. Установить соответствие между средствами и функциями

1	Человек, информация, технические средства	А	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	Б	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)	В	Элементы информационного пространства

4	Применение средств, позволяющих производить с передаваемой, обрабатываемой, создаваемой, уничтожаемой и воспринимаемой информацией задуманные действия	Г	Психологическое воздействие

2. Установить соответствие между информационными ресурсами телекоммуникационных систем и описаниями функционирования элементов

1	Автоматизированные пользовательские системы, которые собирают, хранят, обрабатывают и распространяют информацию	А	Информация
2	Данные во всех формах ввода, хранения, обработки и вывода с помощью информационных систем, в любых формах, которыеиспользуются для принятия управленческих решений	Б	Инфраструктура
3	Средства (аппаратное и программное обеспечение, системы управления базами данных, сеть, мультимедиа, среда, в которой все это функционирует), которые делают возможным работу приложений	В	Персонал
4	Люди (специалисты), требующиеся для планирования, организации, установки, эксплуатации и развития информационных систем и сервисов, нанимаемые по контрактам	Г	Приложения

3. Установить соответствие между терминами и их значениями

1	Информационная операция	А	действия, предпринимаемые с целью затруднить сбор, обработку передачу и хранение информации информационными системами противника при

			защите собственной информации и информационных систем
2	Информационная война	Б	комплексное воздействие (совокупность информационных операций) на систему государственного и военного управления противостоящей стороны, на ее военно-политическое руководство
3	Информационное превосходство	В	способность собирать, обрабатывать и распределять непрерывный поток информации о ситуации, препятствуя противнику делать то же самое
4	Информационное противоборство	Г	проведения мероприятий, направленных против систем управления и принятия решений (Command & Control Warfare, C2W), а также против компьютерных и информационных сетей и систем (Computer Network Attack, CNA)

4. Установить соответствие

1	Системность целевая	А	Подразумевает единство организации всех работ по защите информации и их управления
2	Системность пространственная	Б	Защищенность информации рассматривается как составная часть общего понятия качества информации
3	Системность временная	В	Защищенность основанная на принципе непрерывности функционирования системы защиты
4	Системность организационная	Г	Защищенность рассматривается как увязка вопросов защиты информации

5. Установить соответствие мер защиты информации

1	Правовые	А	Реализуются в виде механических, электрических и электронных устройств,

			предназначенных для препятствования проникновению и доступу потенциального нарушителя к компонентам защиты
2	Морально-этические	Б	Представляют собой организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации аппаратуры телекоммуникаций для обеспечения защиты информации
3	Административные	В	К ним относятся нормы поведения, которые традиционно сложились по мере распространения сетевых и информационных технологий
4	Технические	Г	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	А	Все иные из числа сведений, составляющих государственную тайну
2	К совершенно секретным сведениям следует относить	Б	Такие сведения, распространение которых может нанести ущерб интересам министерства, ведомства или отраслям экономики РФ в одной или нескольких областях деятельности
3	К секретным сведениям следует относить	В	Такие сведения, распространение которых может нанести ущерб интересам РФ в одной или нескольких областях

			деятельности

7. Установить соответствие

1	Нарушитель	А	намеренно идущий на нарушение из корыстных побуждений
2	Злоумышленник	Б	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	В	Лицо, которое с корыстными целями осуществляет несанкционированный доступ к данным или программам

8.Установить соответствие между терминами и их значениями

1	Техническая сфера	А	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	Б	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	В	совокупность людей, организаций и систем, собирающих, отрабатывающих, доводящих информацию или действующих на ее основе

4	Элементы информационной обстановки	Г	руководители, лица, принимающие решения (ЛПР), люди организации и системы

9. Установить соответствие между

1	Перехват паролей	А	мошенничество возможно с участием специальных программ, которые имитируют на экране монитора окошко для ввода имени и пароля. Введенные данные попадают в руки злоумышленника, и далее на дисплее появляется сообщение о неправильной работе системы.
2	«Маскарад»	Б	действия в информационной системе от лица другого человека в сети компании. Существуют такие возможности реализации планов злоумышленников в системе -передача ложных данных в системе от имени другого человека
3	Незаконное использование привилегий	В	название разновидности хищения информации и подрыва безопасности информационной системы говорит само за себя

10. Установить соответствие между типологиями «Информационных войн»

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

11.Установить соответствие уровней информационной борьбы

1	Вещественно-энергетический	А	Борьба на уроне носителей информации, то есть все виды скрытия информации и уничтожения информационных систем каналов и информации в них
2	Синтаксический	Б	Борьба на уровне структур знаковых систем , то есть все виды кодирования , использования шифров и т.п
3	Семантический	В	борьба на уровне смыслового содержания информации, то есть предоставление противнику бессмысленной или недостоверной информации (дезинформация)
4	прагматический	Г	борьба на уровне полезности информации, то есть либо изменения целей противостоящей стороне по отношению к использованию информации, либо предоставление ему бесполезной информации

12.Установить соответствие между терминами и их значениями

1	Ресурсы информационной обстановки	А	материальные средства и системы, используемые для сбора, анализа, применения или доведения информации
2	Информационное измерение	Б	область, в которой создается, обрабатывается и накапливается информация. Кроме того, это область, в которой существует логика функционирования систем управления, связи и разведки. В битве за информационное превосходство эта область является самой чувствительной к информационным воздействиям, так как именно это измерение связывает реальный физический мир с логикой

			функционирования технических систем сбора, передачи и обработки информации, а через них — с сознанием человека, функционирующим в познавательном измерении
3	Познавательное измерение	В	область мышления бойца и мирного населения. Это область, в которой формируются намерения командиров, доктрины, тактика, методы противоборства. Нематериальные активы лидерства, морали, сплоченности подразделений, уровень подготовки, опыта, понимания ситуации и общественного мнения — это всё элементы этой области
4	Физическое измерение	Г	традиционная область войны. Эта область объединяет традиционные сферы противоборства — землю, море, воздух и космическое пространство. Это область, в которой функционируют физические платформы вооружений и технические системы управления и связи. Поэтому элементы этой области проще всего идентифицируемы. Боевая мощь в этой области традиционно измеряется эффектами физического поражения

13. Установить соответствие между излучениями каналов

1	Побочные электромагнитные излучения и наводки (ПЭМИН)	А	паразитные и побочные электромагнитные излучения радиоэлектронного оборудования и средств вычислительной техники. В зависимости от среды распространения различают
2	Побочные электромагнитные	Б	нежелательные (паразитные) электромагнитные излучения,

	излучения (ПЭМИ)		возникающие при функционировании технических средств обработки информации, и приводящие к утечке обрабатываемой информации
3	Информативными ПЭМИ	В	сигналы, представляющие собой ВЧ несущую, модулированную информацией обрабатываемой на СВТ (например, изображением, выводимым на экран монитора, данными, обрабатываемыми на устройствах ввода-вывода и т.д.)
4	Неинформативными ПЭМИ	Г	сигналы, анализ которых может дать представление только о режиме работы СВТ и никак не раскрывает характер информации, обрабатываемой на СВТ

14.Установить соответствие между терминами и их значениями

1	Кибербезопасность	А	набор средств, стратегий, принципов обеспечения безопасности, мер по обеспечению безопасности, руководящих принципов, подходов к управлению рисками, действий, профессиональной подготовки, практического опыта, страхования и технологий, которые могут быть использованы для защиты киберпространства, ресурсов организации и пользователя
2	Киберпространство	Б	среда, которая представляет собой следствие результата взаимодействия людей, программного обеспечения и услуг в Интернете с помощью технологий устройств и сетей, подключенных к ней, которых не существует в какой-либо физической форме
3	Кибернетика	В	наука об оптимальном управлении сложными динамическими системами,

			изучающая общие принципы управления и связи, лежащие в основе работы самых разнообразных по природе систем — от самонаводящихся ракет-снарядов и быстродействующих вычислительных машин до сложного живого организма

15. Установить соответствие между основными принципы защиты информации

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

16. Установить соответствие между терминами и определениями

1	Специальные обследования помещений	А	комплекс мер в области защиты информации в части проведения работ по выявлению электронных устройств, предназначенных для негласного получения сведений в помещениях, где циркулирует

			информация ограниченного пользования
2	Аттестация объекта защиты	Б	официальное подтверждение наличия на объекте защиты необходимых и достаточных условий, обеспечивающих выполнение установленных требований РД по ЗИ
3	Основные технические средства и системы	В	технические средства и системы, а также их коммуникации, используемые для обработки, хранения и передачи конфиденциальной информации
4	Нормирование показателей защищенности	Г	установление нормативными документами численных значений показателей защищенности информации

17. Установить соответствие между элементами и функциями

1	Дробление	А	знание какой-то одной части информации не позволяет восстановить всю технологию в целом
2	Кодирование	Б	метод защиты информации, преследующий цель скрыть от соперника содержание защищаемой информации и заключающийся в преобразовании с помощью кодов открытого текста в условный при передаче информации по каналам связи
3	Шифрование	В	метод защиты информации, используемый при передаче сообщений с помощью различной радиоаппаратуры, направлении письменных сообщений и в других случаях, когда есть опасность перехвата этих сообщений соперником

18. Установить соответствие между элементами и функциями

1	Случайные антенны	А	вспомогательные технические средства, их соединительные линии, а также линии

			электропитания, посторонние проводники и цепи заземления, при непосредственном подключении к которым средств разведки ПЭМИН возможен перехват информационных сигналов
2	Сосредоточенные	Б	телефонный аппарат, громкоговоритель радиотрансляционной сети, датчик пожарной сигнализации и т. д., подключенные к линии, выходящей за пределы КЗ
3	Распределенные	В	кабели, провода, металлические трубы и другие токопроводящие коммуникации, выходящие за пределы КЗ

19. Установить соответствие между терминами и определениями

1	Автоматизированная система (АС)	А	система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функции
2	Контролируемая зона (КЗ)	Б	пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание сотрудников и посетителей организации, а также транспортных, технических и иных материальных средств
3	Специальные исследования (СИ)	В	выявление с использованием контрольно-измерительной аппаратуры возможных каналов утечки защищаемой информации от основных и вспомогательных технических средств и систем
4	Специальная проверка (СП)	Г	проверка технических средств и систем объекта защиты с целью выявления возможно внедренных электронных устройств съема информации (закладочных

			устройств)

20. Установить соответствие классификации угроз

1	Состояние источника угрозы	А	в самой системе, что приводит к ошибкам в работе и сбоям при реализации ресурсов АС; в пределах видимости АС, например, применение подслушивающей аппаратуры, похищение информации в распечатанном виде или кража записей с носителей данных
2	Степень влияния	Б	активная угроза безопасности, которая вносит коррективы в структуру системы и ее сущность, например, использование вредоносных вирусов или троянов; пассивная угроза – та разновидность, которая просто ворует информацию способом копирования, иногда скрытая. Она не вносит своих изменений в информационную систему.
3	Возможность доступа сотрудников к системе программ или ресурсов		вредоносное влияние, то есть угроза информационным данным может реализоваться на шаге доступа к системе (несанкционированного); вред наносится после согласия доступа к ресурсам системы.
4	Способ доступа к основным ресурсам системы	Г	применение нестандартного канала пути к ресурсам, что включает в себя несанкционированное использование возможностей операционной системы; использование стандартного канала для открытия доступа к ресурсам, например, незаконное получение паролей и других параметров с дальнейшей маскировкой под зарегистрированного в системе

			пользователя.

Задания на установление правильной последовательности

1.Установить в историческом порядке этапы развития информационного противоборства:

1. Распространение грамотности, в условиях широкого охвата населения новыми носителями информации: письмами, листовками, книгами, газетами, журналами и др.

2.Использование в качестве объекта воздействия - психику человека (носитель и средство доведения информации – человек).

3. Появление персональных компьютеров и межгосударственных телекоммуникационных сетей, особенно Интернета.

4. Возникновение новых носителей информации и новых средств доставки информации, появившихся благодаря открытию электричества: телеграфа, телефона, радио, кино, телевидения, звукоусилительной аппаратуры и т.п.

2.Установить этапы защиты от угроз безопасности:

1. Предоставление персоналу защищенный удаленный доступ к информационным ресурсам

2. Обеспечение безопасного доступа к открытым ресурсам внешних сетей и Internet

3. Защита внешних каналов передачи информации

4. Разработка политики информационной безопасности

5. Анализ угрозы безопасности

3. Установить этапы стадии исполнения компьютерных вирусов:

1. Выполнение деструктивных функций

2. Передача управления программе-носителю вируса

3. Поиск жертвы

4. Заражение найденной жертвы

5. Загрузка вируса в память

4. Установить этапы построения системы антивирусной защиты сети:

1. Реализация плана антивирусной безопасности

2. Проведение анализа объекта защиты и определение основных принципов обеспечения антивирусной безопасности

3. Разработка политики антивирусной безопасности

4. Разработка плана обеспечения антивирусной безопасности

5. Расположить этапы проведения аудита информационной безопасности:

1. Разработка рекомендаций по повышению уровня защиты автоматизированной системы
2. Анализ полученных данных
3. Сбор исходных данных
4. Разработка регламента проведения аудита

6. Установить этапы построения программы обеспечения безопасности:
1. Проведение разъяснительных мероприятий и обучения персонала для поддержки требуемых мер безопасности
2. Регулярный контроль пошаговой реализации плана безопасности
3. Установление уровня безопасности
4. Формирование политики безопасности организации
5. Определение ценности технологических и информационных активов организации

7. Установить действия этапа анализа рисков:
1. Оценка вероятности того, что угроза будет реализована на практике
2. Оценка рисков технологических и информационных активов
3. Идентификация и оценка стоимости технологических и информационных активов
4. Анализ угроз, для которых технологические и информационные активыявляются целевым объектом

8. Установить последовательность процессов для обнаружения и выдачи сигнала тревоги:
1. Одно системное событие не является неизбежно достаточным, чтобы утверждать, что это опасность
2. Если результат этой совокупности превышает пороговую величину, выдается сигнал тревоги
3. Совокупность событий должна сравниваться с заранее установленной пороговой величиной
4. Каждое нарушение безопасности должно генерировать системное событие

9. Расположить параметры для группировки данных на сервере сбора информации об атаке:
1. Дата, время
2. Протокол
3. Порт получателя
4. Номер агента
5. IP-адрес атакующего
6. Тип атаки

10. Расположить в порядке возрастания даты разработки стандартов информационной безопасности:

1. ISO 27001:2005
2. ISO/IEC 17799
3. ISO/IEC 15408
4. «Критерии оценки доверенных компьютерных систем»

11. Расположить этапы процесса управления рисками информационной безопасности:

1. Классификация рисков, выбор методологии оценки рисков и проведение оценки
2. Анализ угроз и их последствий, определение слабостей в защите
3. Выбор, реализация и проверка защитных мер
4. Оценка остаточного риска
5. Идентификация активов и ценности ресурсов, нуждающихся в защите
6. Выбор анализируемых объектов и степени детальности их рассмотрения

12. 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

13.Выделите по важности 3 части информационного противоборства

1.Стратегический анализ
2.Информационное воздействие
3.Информационное противодействие

14. 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

15.Расположите по порядку основные формы информационного противоборства

1.информационное доминирование
2.информационная асимметрия
3.информационное сдерживание

4.информационная агрессия
5.контроль и управление информацией

16. 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.

17. Выберите последовательность уровней защищенности персональных данных

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

18. 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.

19. 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.

20. Устранение уязвимости состоит из следующих этапов:

1. Инсталляция программного модуля для устранения угрозы информационной безопасности.

2. Разработка «патча» (заплатки), призванного устранить существующий пробел.

3. Появление сигнала от пользователей или от администратора сети о наличии слабого места в информационной системе.

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.