Энгельсский технологический институт (филиал) федерального государственного
бюджетного образовательного учреждения
высшего образования
«Саратовский государственный технический университет
имени Гагарина Ю.А.»

Кафедра «Естественные и математические науки»

Оценочные материалы по дисциплине
по дисциплине

Б.1.1.14 «Защита информации»

направления подготовки
09.03.04 «Программная инженерия»

профиль
«Управление разработкой программных проектов»

Энгельс 2025

1. Перечень компетенций и уровни их сформированности по дисциплинам (модулям), практикам в процессе освоения ОПОП ВО

В процессе освоения образовательной программы у обучающегося в ходе изучения дисциплины «Защита информации» должны сформироваться компетенции:

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.

Критерии определения сформированности компетенций на различных уровнях их формирования

Индекс компетенции	Содержание компетенции
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности

Код и наименование индикатора достижения компетенции	Виды занятий для формирования компетенции	Оценочные средства для оценки уровня сформированности компетенции
ИД-1$_{ОПК-3}$ Решает задачи диагностики и настройки активного сетевого оборудования	Практические занятия Лекции Самостоятельная работа студентов	Устный опрос, вопросы для проведения зачета, экзамена, тестовые задания

Уровни освоения компетенции

Уровень освоения компетенции	Критерии оценивания
Продвинутый (отлично)	**знает**: показывает всестороннее, систематическое и глубокое знание роли информации в жизни современного общества, понятие информационного общества, его основные признаки; основные нормативные акты в области информационной безопасности; источники и классификацию угроз безопасности компьютерной информации; основные методы обеспечения информационной безопасности; основные нормативные акты в области информационной безопасности **умеет**: на высоком уровне освоения демонстрирует умение пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; составлять аналитические обзоры

	по вопросам обеспечения информационной безопасности; использовать нормативно-правовые документы в области информационной безопасности **владеет**: при выполнении заданий свободно владеет навыками анализа и систематизации информации в области информационной безопасности; навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
Повышенный (хорошо)	**знает**: показывает с отдельными пробелами знание роли информации в жизни современного общества, понятие информационного общества, его основные признаки; основные нормативные акты в области информационной безопасности; источники и классификацию угроз безопасности компьютерной информации; основные методы обеспечения информационной безопасности; основные нормативные акты в области информационной безопасности **умеет**: с отдельными пробелами демонстрирует умение пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; использовать нормативно-правовые документы в области информационной безопасности **владеет**: с отдельными пробелами владеет навыками анализа и систематизации информации в области информационной безопасности; навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
Пороговый (базовый) (удовлетворительно)	**знает**: показывает в неполном объеме знание роли информации в жизни современного общества, понятие информационного общества, его основные признаки; основные нормативные акты в области информационной безопасности; источники и классификацию угроз безопасности компьютерной информации; основные методы обеспечения информационной безопасности; основные нормативные акты в области информационной безопасности **умеет**: в неполном объеме демонстрирует умение пользоваться современной научно-технической информацией по исследуемым проблемам и задачам; составлять аналитические обзоры по вопросам обеспечения информационной безопасности; использовать нормативно-правовые документы в области информационной безопасности **владеет**: в неполном объеме владеет навыками анализа и систематизации информации в области информационной безопасности; навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

2. Методические, оценочные материалы и средства, определяющие процедуры оценивания сформированности компетенций (элементов компетенций) в процессе освоения ОПОП ВО

2.1 Оценочные средства для текущего контроля

Вопросы для устного опроса

Тема 1. Введение в предмет.

Предмет защиты (информация – определение, свойства: важность, ценность; жизненный цикл, виды и формы представления)

Тема 2. Основные понятия информационной безопасности.

Документы, регламентирующие деятельность по ее обеспечению; задачи информационной безопасности; классификация методов защиты; методы, лежащие в основе атак, и каналы утечки информации.

Тема 3. Средства защиты от несанкционированного доступа.

Обзор рынка программно-аппаратных комплексов защиты информации.

Тема 4. Технические аспекты обеспечения информационной безопасности вычислительных систем.

Излучения ПЭВМ, параметры информационно-опасных сигналов, экранирование каналов утечек информации,

экранирование помещений.

Тестовые задания для текущего контроля

2.2 Оценочные средства для промежуточного контроля

1 Вставьте пропущенное слово:

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

а) поддерживающей инфраструктуры

б) человека

в) конфиденциальных данных

2 Защита информации – это …

а) комплекс мероприятий, направленных на обеспечение информационной безопасности

б) совокупность методов, средств и мер, направленных на обеспечение информационной безопасности общества, государства и личности во всех областях их жизненно важных интересов

в) комплекс мероприятий, проводимых собственником информации, по ограждению своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к засекреченной информации и ее носителям

г) все определения корректны

3 Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются:

а) обнаружение угроз

б) пресечения и локализация угроз

в) ликвидация угроз

4 Возможность за приемлемое время получить требуемую информационную услугу называется:

а) доступностью информации

б) целостностью информации

в) предоставлением информации

5 Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения называется:

а) доступностью информации

б) целостностью информации

в) предоставлением информации

г) конфиденциальностью информации

6 Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации

а) доступность информации

б) целостность информации

в) предоставление информации

г) конфиденциальность информации

7 Меры каких уровней НЕ входят в организацию системы обеспечения информационной безопасности:

а) законодательного уровня

б) административного уровня

в) процедурного уровня

г) программно-технического уровня

д) программно-аппаратного уровня

8 Какие из перечисленных ниже угроз относятся к классу преднамеренных? а) заражение компьютера вирусами

б) физическое разрушение системы в результате пожара

в) отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т.п.)

г) проектирование архитектуры системы, технологии обработки данных, разработка

прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации
д) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств
е) вскрытие шифров криптозащиты информации

9 Вопросы сертификации и лицензирования средств обеспечения информационной безопасности в России рассматривает:

а) Федеральная служба по техническому и экспортному контролю при Президенте РФ
б) Федеральная служба безопасности Российской Федерации
в) Служба внешней разведки Российской Федерации

10 Совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов принято считать:

а) политикой безопасности
б) методами защиты информации
в) ограничением доступа к информации
г) учетными записями пользователей

11 Потенциальная возможность определенным образом нарушить информационную безопасность – это ….

а) угроза
б) атака
в) взлом

12 Некоторая уникальная информация, позволяющая различать пользователей называется:

а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ

13 Некоторая секретная информация, известная только пользователю и парольной системе, которая может быть запомнена пользователем и предъявлена парольной системе называется:

а) идентификатор (логин)
б) пароль
в) учетная запись
г) ключ

14 Совокупность идентификатора и пароля пользователя называется:

а) логин пользователя
б) учетная запись пользователя
в) ключ пользователя

15 Присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных является:

а) идентификацией пользователя
б) аутентификацией пользователя

в) опознанием пользователя
г) созданием учетной записи пользователя

16 Проверка принадлежности пользователю предъявленного им идентификатора является:

а) идентификацией пользователя
б) аутентификацией пользователя
в) регистрацией пользователя
г) созданием учетной записи пользователя

17 Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) перехват передаваемой по сети информации (Sniffing)
д) спуфинг
е) сканирование портов

18 Атака, целью которой является трафик локальной сети, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

19 Атака, целью которой являются логины и пароли пользователей, атака проходит путем имитации приглашения входа в систему или регистрации для работы с программой, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

20 Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется:

а) «Отказ от обслуживания» (Denial of Service - DoS)
б) срыв стека
в) внедрение на компьютер деструктивных программ
г) снифинг (Sniffing)
д) спуфинг
е) сканирование портов

21 Разработка нормативных правовых актов, регламентирующих

отношения в информационной сфере, и нормативных методических документов по вопросам обеспечения информационной безопасности РФ относится к:

а) правовым методам защиты информации

б) организационно-техническим методам защиты информации

в) организационно-распорядительным методам защиты информации

г) инженерно-технической защите

22 Контроль за выполнением специальных требований по защите информации относится к:

а) правовым методам защиты информации

б) организационно-техническим методам защиты информации

в) организационно-распорядительным методам защиты информации

г) экономическим методам защиты информации

23 Создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи относится к:

а) правовым методам защиты информации

б) организационно-техническим методам защиты информации

в) организационно-распорядительным методам защиты информации

г) экономическим методам защиты информации

24 Разработкапрограмм обеспечения информационной безопасности РФ и определение порядка их финансирования относится к:

а) правовым методам защиты информации

б) организационно-техническим методам защиты информации

в) организационно-распорядительным методам защиты информации

г) нормативно-правовым методам защиты информации

д) экономическим методам защиты информации

25 Регулирование вопросов, связанных с защитой имущественных, авторских (неимущественных) и иных интересов собственников информации относят к:

а) правовым методам защиты информации

б) организационно-техническим методам защиты информации

в) организационно-распорядительным методам защиты информации

г) нормативно-правовым методам защиты информации

д) экономическим методам защиты информации

26 Субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения информацией, называется:

а) собственник информации

б) владелец информации

в) пользователь

27 К какому виду конфиденциальной информации относится научно-техническая, технологическая, производственная, финансово-экономическая и

иная деловая информация, в том числе информация о секретах производства?
а) коммерческая тайна
б) персональные данные
в) государственная служебная тайна
г) процессуальная тайна
28 К какому виду конфиденциальной информации относятся сведения, которые могут стать известными в ходе расследования преступлений и правонарушений, при проведении криминалистических экспертиз, при заслушивании дел в суде?
а) коммерческая тайна
б) персональные данные
в) государственная служебная тайна
г) процессуальная тайна
29 Особая категория информации, основной задачей защиты которой является охрана прав человека, который является создателем, называется:
а) коммерческая тайна
б) персональные данные
в) процессуальная тайна
г) авторское или патентное право
30 Противоправные процессы утечки, утраты, распространения, разглашения, копирования, тиражирования, фальсификации, хранения с целью передачи, удаления информации называется процессом:
а) незаконного оборота информации
б) взлома информации
в) несанкционированного использования информации
31 Какое направление защиты в основном применяется для охраны материальных ценностей?
а) инженерно-техническая
б) организационно-техническая
в) организационно-распорядительная
г) нормативно-правовая
д) экономическая
32 Что из нижеперечисленного оборудования может выступать в качестве технического канала связи?
а) контроллер жесткого диска, передающий электрические импульсы, считанные магниторезистивной головкой с поверхности магнитного носителя, по шлейфу в системную магистраль для копирования в оперативную память
б) инфракрасный светодиод лазерного принтера, посылающий кратковременные
вспышки на электризованную поверхность фоточувствительного барабана
в) модулированный по силе тока поток электронов, засвечивающий в определенном порядке пиксели люминофора электронно-лучевой трубки
г) экран компьютерного монитора и глаза пользователя д) оптический канал связи
е) все варианты могут быть отнесены к техническим каналам связи

33 Какой канал утечки информации основан на использовании электромагнитной энергии видимого и инфракрасного диапазона?

а) визуально-оптический канал

б) электромагнитный канал

в) виброакустический канал

г) материально-вещественный канал

34 Процесс перехвата и фиксации процесса клавиатурного ввода идентифицирующей информации является примером утечки информации:

а) визуально-оптического канала

б) электромагнитного канала

в) виброакустического канала

г) материально-вещественного канала

35 Процесс разведки за объектами на территории другого государства с космических аппаратов является примером утечки информации:

а) визуально-оптического канала

б) электромагнитного канала

в) виброакустического канала

г) материально-вещественного канала

36 Какой канал утечки информации включает в себя весь радиодиапазон от сверхнизких до сверхвысокочастотных волн?

а) визуально-оптический канал

б) электромагнитный канал

в) виброакустический канал

г) материально-вещественный канал

37 Электрические сигналы (напряжения, токи), модулированные по закону передаваемого сообщения, протекающие по проводникам и элементам радиоцепей (линиям связи, антеннам, конденсаторам) и возбуждающие в окружающем пространстве электромагнитную энергию является примером утечки информации:

а) визуально-оптического канала

б) электромагнитного канала

в) виброакустического канала

г) материально-вещественного канала

38 Какой канал утечки информации представляет собой фактический побочный прием модулированной акустической энергии, распространяющейся в газообразной, жидкой или твердой средах

а) визуально-оптический канал

б) электромагнитный канал

в) виброакустический канал

г) материально-вещественный канал

39 Примером какого канала утечки информации служит звук голоса человека?

а) визуально-оптического канала

б) электромагнитного канала

в) виброакустического канала
г) материально-вещественного канала

40 Выбрасывание на свалки отходов производства, низкая дисциплина при распечатке и размножении конфиденциальных документов, пренебрежение правилами учета, хранения и уничтожения вещественных носителей информации создают предпосылки для использования противником канала утечки информации …

а) визуально-оптического канала
б) электромагнитного канала
в) виброакустического канала
г) материально-вещественного канала

41 Установление подлинности идентифицированного пользователя – это ...

а) санкционирование
б) авторизация
в) аутентификация
г) идентификация

42 Процедура опознавания пользователя по предъявленному идентификатору – это …

а) санкционирование
б) авторизация
в) аутентификация
г) идентификация

43 Некое уникальное количество информации, позволяющее различать субъекты и объекты доступа – это …

а) идентификатор
б) пароль
в) учетная запись
г) регистрация

44 Процедура ввода идентифицирующей и аутентифицирующей информации с протоколированием действий – это …

а) идентификатор
б) пароль
в) учетная запись
г) регистрация

45 Из каких двух этапов состоит процедура распознавания личности?

а) регистрация
б) идентификация
в) аутентификация
г) реагирование

46 Какой из этапов распознавания личности проходит первым?

а) идентификация
б) аутентификация
в) авторизация

47 Парольная информация, известная только пользователю и проверяющей

системе нужна пользователю для прохождения процедуры:
а) регистрации
б) идентификации
в) аутентификации
г) реагирования

48 Уникальный индивидуальный признак, свойственный лишь этому пользователю (голос, отпечаток пальца) нужен пользователю для прохождения процедуры:
а) регистрации
б) идентификации
в) аутентификации
г) реагирования

49 Самый хороший пароль становится плохим, если:
а) записать его где-нибудь в открытом месте
б) набирать его в присутствии посторонних
в) забыть его
г) все варианты подходят для того, чтобы испортить хороший пароль

50 Сколько выделяются основных составляющих национальных интересов Российской Федерации в информационной сфере?
а) 2
б) 3
в) 4
г) 5
д) 6

51 Сертификации подлежат:
а) средства криптографической защиты информации
б) средства выявления закладных устройств и программных закладок
в) защищенные технические средства обработки информации
г) защищенные информационные системы и комплексы телекоммуникаций д) все вышеперечисленные средства

52 Среди нижеперечисленных выделите главную причину существования многочисленных угроз информационной безопасности:
а) просчеты при администрировании информационных систем
б) необходимость постоянной модификации информационных систем
в) сложность современных информационных систем

53 Уголовный кодекс РФ не предусматривает наказания за:
а) создание, использование и распространение вредоносных программ
б) ведение личной корреспонденции на производственной технической базе
в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

54 Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:
а) средства выявления злоумышленной активности
б) средства обеспечения отказоустойчивости
в) средства контроля эффективности защиты информации

55 Политика безопасности строится на основе:

а) общих представлений об ИС организации

б) изучения политик родственных организаций

в) анализа рисков

56 Действие Закона "О лицензировании отдельных видов деятельности" распространяется на:

а) деятельность по использованию шифровальных (криптографических) средств

б) деятельность по рекламированию шифровальных (криптографических) средств

в)деятельность по распространению шифровальных (криптографических) средств

57 Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:

а) средства выявления злоумышленной активности

б) средства обеспечения отказоустойчивости

в) средства контроля эффективности защиты информации

58 Действие Закона "О лицензировании отдельных видов деятельности" не распространяется на:

а) деятельность по технической защите конфиденциальной информации

б) образовательную деятельность в области защиты информации

в) предоставление услуг в области шифрования информации

59 Под определение средств защиты информации, данное в Законе "О государственной тайне", подпадают:

а) средства выявления злоумышленной активности

б) средства обеспечения отказоустойчивости

в) средства контроля эффективности защиты информации

60 Что представляет собой Доктрина информационной безопасности РФ?

а) нормативно-правовой акт, устанавливающий ответственность за правонарушения в сфере информационной безопасности

б) федеральный закон, регулирующий правоотношения в области информационной безопасности

в) целевая программа развития системы информационной безопасности РФ, представляющая собой последовательность стадий и этапов

г) совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации

Вопросы к зачету:

1. Виды безопасности и сферы жизнедеятельности личности, общества и государства.
2. Определение информационной безопасности.
3. Функции и объекты защиты информации.
4. Степени секретности информации.
5. Субъекты и причины совершения компьютерных преступлений.
6. Уровни информационной защиты.
7. Ответственность за нарушение информационной безопасности.
8. Принципы информационной безопасности.

9. Определение конфиденциальности, целостности, доступности информации.

10. Предмет криптографии. Определения. Задачи. Исторические примеры.

11. Виды атак на криптографические алгоритмы. Понятие стойкости.

12. Классификация алгоритмов шифрования. Примеры простейших шифров.

13. Шифры замены.

14. Шифры перестановки.

15. Шифры гаммирования.

16. Проблемы и особенности защиты информации в компьютерных сетях.

17. Виды угроз информационной безопасности. Основные нарушения.

18. Характер происхождения угроз.

19. Источники угроз (непосредственный исполнитель угрозы в плане ее негативного воздействия на информацию).

20. Классы каналов несанкционированного получения информации.

21. Классификация методов и средств обеспечения безопасности

22. Методы обеспечения безопасности сетей

23. Понятие актуальности угрозы безопасности.

24. Понятие модели угроз. Этапы проведения оценки угроз безопасности.

25. Основные нормативные документы, необходимые для составления модели угроз.

26. Понятие нарушителя. Типы нарушителей, их возможности и цели (по методическому документу ФСТЭК «Методика оценки угроз безопасности информации» от 05.02.2021).

27. Определение средств защиты информации (СЗИ).

28. Классификация средств защиты информации.

29. Инженерно-техническая защита информации.

30. Физические средства защиты.

31. Аппаратные средства защиты.

32. Программные средства защиты.

33. Криптографические средства защиты информации.

34. Встроенные средства защиты операционных систем (ОС).

35. Идентификация и аутентификация.

36. Управление доступом.

37. Протоколирование и аудит.

38. Антивирусная защита. Методы антивирусной защиты. Виды антивирусных программ.

39. Межсетевые экраны. Основные компоненты и технологии.

40. Недостатки, связанные с применением межсетевого экрана.

41. VPN. Классификация VPN сетей.

42. Принципы построения VPN сетей. VPN на базе брэндмауэров, VPN на базе маршрутизаторов, VPN на базе программного обеспечения. VPN на базе аппаратных средств.

43. Протоколы VPN сетей. Методы реализацииVPN сетей (туннелирование, аутентификация, шифрования).

44. Определение прокси-сервера. Цели применения прокси-сервера. Виды прокси-серверов.

45. Система обнаружения вторжений (IDS). Классификация IDS.

46. Архитектура IDS.

47. Перечислить основные элементы локальной архитектуры систем обнаружения вторжений.

48. Глобальная архитектура систем обнаружения вторжений.

49. Система предотвращения вторжений.

50. Перечислить цели использования IPS-систем.

51. Классификация IPS-систем.

52. Криптографические средства защиты информации.

53. Перечислить требования, предъявляемые к криптосистемам.

54. Раскрыть понятие «электронная подпись».

Оценивание результатов обучения в форме уровня сформированности элементов компетенций проводится путем контроля во время промежуточной аттестации в форме зачета:

а) оценка «зачтено» – компетенция(и) или ее часть(и) сформированы на базовом уровне;

б) оценка «не зачтено» – компетенция(и) или ее часть(и) не сформированы.

Критерии, на основе которых выставляются оценки при проведении текущего контроля и промежуточной аттестации приведены в табл. 1.

Оценки «Не зачтено» ставятся также в случаях, если обучающийся не приступал к выполнению задания, а также при обнаружении следующих нарушений:

– списывание;

– плагиат;

– фальсификация данных и результатов работы.

Таблица 1 – Критерии выставления оценок при проведении текущего контроля и промежуточной аттестации

Шкала оценки	Оценка	Критерий выставления оценки
Двухбалльная шкала	Зачтено	Обучающийся ответил на теоретические вопросы. Показал знания в рамках учебного материала. Выполнил практические задания. Показал удовлетворительные умения и владения навыками применения полученных знаний и умений при решении задач в рамках учебного материала
	Не зачтено	Обучающиеся при ответе на теоретические вопросы и при выполнении практических заданий продемонстрировал недостаточный уровень знаний и умений при решении задач в рамках учебного материала. При ответах на дополнительные вопросы было допущено множество неправильных ответов

2.3. Итоговая диагностическая работа по дисциплине

ЗАДАНИЯ ДЛЯ ДИАГНОСТИЧЕСКОЙ РАБОТЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ), ПРАКТИКЕ

Номер задания	Правильный ответ *	Содержание вопроса	Компетенция
1.		Защита информации – это	ОПК-3
2.		Информационная безопасность - это	ОПК-3
3.		Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются …	ОПК-3
4.		Выбрасывание на свалки отходов производства, низкая дисциплина при распечатке и размножении конфиденциальных документов, пренебрежение правилами учета, хранения и уничтожения вещественных носителей информации создают предпосылки для использования противником	ОПК-3
5.		Установление подлинности идентифицированного пользователя – это	ОПК-3
6.		Нарушение какого из аспектов информационной безопасности влечет за собой искажение официальной информации, например, текста закона, выложенного на странице Web-сервера какой-либо правительственной организации	ОПК-3
7.		Потенциальная возможность определенным образом нарушить информационную безопасность – это ….	ОПК-3
8.		Проверка принадлежности пользователю предъявленного им идентификатора является…	ОПК-3
9.		К какому виду конфиденциальной информации относится научно-техническая, технологическая, производственная, финансово-экономическая и иная деловая информация, в том числе информация о	ОПК-3
10.		Примером какого канала утечки информации служит звук голоса человека?	ОПК-3
11.	а	Действия по определению конкретных угроз и их источников, приносящих тот или иной вид ущерба называются: а) обнаружение угроз б) пресечения и локализация угроз в) ликвидация угроз	ОПК-3

12.	а	Установление подлинности идентифицированного пользователя – это ... а) санкционирование б) авторизация в) аутентификация г) идентификация	
13.	в	Парольная информация, известная только пользователю и проверяющей системе нужна пользователю для прохождения процедуры: а) регистрации б) идентификации в) аутентификации г) реагирования	ОПК-3
14.	а	Атака на ресурс, которая вызывает нарушение корректной работы программного или аппаратного обеспечения, путем создания огромного количества фальшивых запросов на доступ к некоторым ресурсам или путем создания неочевидных препятствий корректной работе называется: а) «Отказ от обслуживания» (Denial of Service - DoS) б) срыв стека в) внедрение на компьютер деструктивных программ г) перехват передаваемой по сети информации (Sniffing) д) спуфинг е) сканирование портов	ОПК-3
15.	б	Совокупность идентификатора и пароля пользователя называется: а) логин пользователя б) учетная запись пользователя в) ключ пользователя	ОПК-3
16.	д	Сертификации подлежат: а) средства криптографической защиты информации б) средства выявления закладных устройств и программных закладок в) защищенные технические средства обработки информации г) защищенные информационные системы и комплексы телекоммуникаций д) все вышеперечисленные средства	ОПК-3
17.	г	Особая категория информации, основной задачей защиты которой является охрана прав человека, который является создателем, называется: а) коммерческая тайна б) персональные данные	ОПК-3
		в) процессуальная тайна г) авторское или патентное право	

18.	в	Уникальный индивидуальный признак, свойственный лишь этому пользователю (голос, отпечаток пальца) нужен пользователю для прохождения процедуры: а) регистрации б) идентификации в) аутентификации г) реагирования	ОПК-3
19.	е	Сетевая атака, целью которой является поиск открытых портов работающих в сети компьютеров, определение типа и версии ОС и ПО, контролирующего открытый порт, используемых на этих компьютерах, называется: а) «Отказ от обслуживания» (Denial of Service - DoS) б) срыв стека в) внедрение на компьютер деструктивных программ г) снифинг (Sniffing) д) спуфинг е) сканирование портов	ОПК-3
20.	в	Политика безопасности строится на основе: а) общих представлений об ИС организации б) изучения политик родственных организаций в) анализа рисков	ОПК-3