МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ

ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

Фонды оценочных средств по дисциплине «ПРАВОВЫЕ И ОРГАНИЗАЦИОННЫЕ ОСНОВЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

1. Формируемые дисциплиной компетенции

ОПК.5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации
Индикаторы:
ОПК.5.1 Ориентируется в нормативных правовых актах, нормативных и методически документах, регламентирующих деятельность по защите информации
ОПК.5.2 Применяет на практике знание нормативных правовых актов, нормативных и методически документов, регламентирующих деятельность по защите информации
ОПК.6 Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
Индикаторы:
ОПК.6.1 Ориентируется в нормативных правовых актах и нормативных методических документах Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК.6.2 Определяет необходимые для решения профессиональной задачи нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК.6.3 Организует защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.

Коды компетенций	**Планируемый результат**
ОПК.5.1	Уметь ориентироваться в нормативных правовых актах, нормативных и методических документах, регламентирующих деятельность по защите информации
ОПК.5.2	Знать правовые и организационные методы защиты в автоматизированных системах. уметь применять требования нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации
ОПК.6.1	Знает основные положения нормативных правовых актов и нормативных методических документов Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
ОПК.6.2	Знать нормативные правовые акты и нормативные методические документе Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Уметь выбирать нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю для решения правовых задач.

ОПК.6.3	Знать нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю по защите информации ограниченного доступа в компьютерных системах и сетях. Уметь организовывать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному

3. Спецификация теста

Тест по дисциплине «Правовые и организационные основы обеспечения информационной безопасности» представляет собой перечень примерных вопросов, предлагаемых студентам с учетом тем и заданий для контрольных мероприятий, предусмотренных по дисциплине.

Тест по дисциплине «Организационно-правовое обеспечение информационной безопасности», вариант 1.

1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...
А) политическая разведка;
Б) промышленный шпионаж;
В) добросовестная конкуренция;
Г) конфиденциальная информация;
Д) правильного ответа нет.

2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности?
А) любая информация;
Б) только открытая информация;
В) запатентованная информация;
Г) закрываемая собственником информация;
Д) коммерческая тайна.

3. Кто может быть владельцем защищаемой информации?
А) только государство и его структуры;
Б) предприятия акционерные общества, фирмы;
В) общественные организации;
Г) только вышеперечисленные;
Д) кто угодно.

4. Какие сведения на территории РФ могут составлять коммерческую тайну?
А) учредительные документы и устав предприятия;
Б) сведенья о численности работающих, их заработной плате и условиях труда;
В) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;
Г) другие;
Д) любые.

5. Какие секретные сведения входят в понятие «коммерческая тайна»?
А) связанные с производством;
Б) связанные с планированием производства и сбытом продукции;
В) технические и технологические решения предприятия;
Г) только 1 и 2 вариант ответа;
Д) три первых варианта ответа.

6. Что называют источником конфиденциальной информации?
А) объект, обладающий определенными охраняемыми сведениями, представляющими интерес для злоумышленников;
Б) сведения о предметах, объектах, явлениях и процессах, отображаемые на каком-либо носителе;
В) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники;
Г) это защищаемые предприятием сведения в области производства и коммерческой деятельности;
Д) способ, позволяющий нарушителю получить доступ к обрабатываемой или хранящейся в ПЭВМ информации.

7. Как называют процессы обмена информацией с помощью официальных, деловых документов?
А) непосредственные;
Б) межличностные;
В) формальные;
Г) неформальные;
Д) конфиденциальные.

8. Какое наиболее распространенное действие владельца конфиденциальной информации, приводит к неправомерному овладению ею при минимальных усилиях со стороны злоумышленника?
А) хищение носителей информации;
Б) использование технических средств для перехвата электромагнитных ПЭВМ;
В) разглашение;
Г) копирование программой информации с носителей;
Д) другое.

9. Каким образом происходит разглашение конфиденциальной информации?
А) утеря документов и других материалов, или пересылка их посредством почты, посыльного, курьера;
Б) опубликование материалов в печати;
В) сообщение, передача, предоставление в ходе информационного обмена;
Г) все вышеперечисленные способы;
Д) правильного варианта ответа нет.

10. Какие основные цели преследует злоумышленник при несанкционированном доступе к информации?
А) получить, изменить, а затем передать ее конкурентам;
Б) размножить или уничтожить ее;
В) получить, изменить или уничтожить;
Г) изменить и уничтожить ее;
Д) изменить, повредить или ее уничтожить.

11. Какой самый прямой и эффективный способ склонения к сотрудничеству?
А) психическое давление;
Б) подкуп;
В) преследование;
Г) шантаж;
Д) угрозы.

12. Наиболее сложный и дорогостоящий процесс несанкционированного доступа к источникам конфиденциальной информации?
А) инициативное сотрудничество;
Б) выпытывание;
В) наблюдение;
Г) хищение;
Д) копирование.

13. Какое из утверждений неверно?
А) подкуп - сложный процесс, требует долгой и кропотливой работы;
Б) выпытывание - это стремление путем внешне наивных вопросов получить определенные сведения;
В) процесс наблюдения не сложен, так как не требует затрат сил и средств;
Г) под незаконным подключением понимают контактное или бесконтактное подсоединение к линиям и проводам с целью несанкционированного доступа к информации, образующейся или передаваемой в них;

Д) негласное ознакомление - способ получения информации, к которой субъект не допущен, но при определенных условиях он может получить возможность кое-что узнать.

14. Завершающим этапом любого сбора конфиденциальной информации является...
А) копирование;
Б) подделка;
В) аналитическая обработка;
Г) фотографирование;
Д) наблюдение.

15. Как называются реальные или потенциально возможные действия или условия, приводящие к овладению, хищению, искажению, изменению или уничтожению информации?
А) ненадежность;
Б) угроза;
В) несчастный случай;
Г) авария;
Д) правильного ответа среди перечисленных нет.

16. Что в скором времени будет являться главной причиной информационных потерь?
А) материальный ущерб, связанный с несчастными случаями;
Б) кража и преднамеренная порча материальных средств;
В) информационные инфекции;
Г) аварии и выход из строя аппаратуры, программ и баз данных;
Д) ошибки эксплуатации.

17. В каком варианте ответа инфекции расположены от более простого к более сложному, по возрастанию?
А) логические бомбы, троянский конь, червь, вирус;
Б) червь, вирус логические бомбы, троянский конь;
В) червь логические бомбы вирус, троянский конь;
Г) логические бомбы, вирус, троянский конь червь;
Д) вирус, логические бомбы, троянский конь червь.

18. Причины, связанные с информационным обменом приносящие наибольшие убытки?
А) остановка или выход из строя информационных систем;
Б) потери информации;
В) неискренность;
Г) проникновение в информационную систему;
Д) перехват информации.

19. Какие цели преследуются при активном вторжении в линии связи?
А) анализ информации (содержание сообщений, частоту их следования и факты прохождения, пароли, идентификаторы коды) и системно-структурный анализ;
Б) воздействие на поток сообщений (модификация, удаление и посылка ложных сообщений) или восприпятствие передаче сообщений;
В) инициализация ложных соединений;
Г) варианты 1 и 2;
Д) варианты 2 и 3.

20. Что определяет модель нарушителя?
А) категории лиц, в числе которых может оказаться нарушитель;
Б) возможные цели нарушителя и их градации по степени важности и опасности;
В) предположения о его квалификации и оценка его технической вооруженности;
Г) ограничения и предположения о характере его действий;
Д) все выше перечисленные.

Тест по дисциплине «Организационно-правовое обеспечение информационной безопасности», вариант 2.

1. Состояние защищенности человека, общества и государства в информационной сфере это
А) Система обеспечения информационной
безопасности Б) Информационная безопасность
В) Национальная безопасность Российской
Федерации Г) Кибербезопасность

2. Обеспечение национальных интересов РФ НЕ осуществляется посредством реализации стратегических национальных приоритетов
А) Обороны страны
Б) Экономический рост
В) Культура
Г) Духовенство

3. Информационная безопасность определяется способностью государства, общества, личности
А) вырабатывать личностные и групповые навыки и умения безопасного поведения
Б) обеспечения криптографической защиты передаваемых по телекоммуникационной системе конфиденциальных сведений и решения вопросов безопасности шифровальной связи
В) реализовывать методы, необходимые для адекватного и наиболее эффективного решения всех задач защиты и содержащие как общеметодологические подходы к решению, так и конкретные прикладные методы решения
Г) вырабатывать научно обоснованные предложения по обеспечению работ по защите информации

4. Что относится к интересам общества?
А) Обеспечение прав на получение информации
Б) Информационное обеспечение государственной политики
В) Защита государственных информационных
ресурсов Г) Обеспечение безопасности ИТКС

5. К внешним источникам угроз в соответствии с Доктриной информационной безопасности Российской Федерации относится:
А) деятельность иностранных политических, экономических, военных, разведывательных и информационных структур против интересов РФ
Б) недостаточный уровень развития конкурентоспособных информационных технологи
В) недостаточная эффективность научных исследований направленных на создание перспективных информационных технологий, низкий уровень внедрения отечественных разработок;
Г) недостаточное кадровое обеспечение в области информационной безопасности

6. К угрозам информационной безопасности личности относится:
А) информационно-психологическая агрессия
Б) нарушение прав в сфере оборота информации (утечка, перехват, хищение, навязывание ложной информации)
В) деструктивное информационно-психологическое воздействие, в условиях действия которого человек полностью или частично утрачивает способность полноценно развиваться
Г) неисполнение требований законов РФ

7. Федеральные законы относятся к
А) Организационно-распорядительные документы Б) Нормативные и методические документы
В) Специальные нормативные документы Г) Нормативные правовые акты

8. Федеральный закон РФ от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». В законе получили закрепления вопросы:
А) отношений, связанных с поиском с применением информационных технологий Б) отношения по отнесению сведений к государственной тайне
В) отношения в области использования электронных подписей
Г) отношения, связанные с отнесением информации к коммерческой тайне

9. Что НЕ является принципом засекречивания сведений и отнесения их к государственной тайне:
А) Законность
Б) Обоснованность
В) Постоянность
Г) Своевременность

10. Возможно ли использование грифов секретности для засекречивания сведений, не отнесенных к государственной тайне?
А) Возможно для любых сведений
Б) Возможно только для коммерческой тайны
В) Возможно для сведений, относящихся к любому другому виду тайны Г) Невозможно

11. Сведения, относящиеся к коммерческой тайне
А) Условия труда
Б) Технология производства
В) Состав имущества предприятия Г) Состав работников

12. Что относится к общим мерам обеспечения соблюдения конфиденциальности информации?
А) разработка перечня информации, относящейся к коммерческой тайн Б) ограничение и регламентирование доступа к носителям информации
В) определение круга лиц, имеющих права доступа к информации Г) верны все варианты
13. Какой класс задач относится к цели обеспечения ИБ «Обеспечение защиты системы от обнаружения»?
А) Регистрац
ия Б)
Маскировка

В) Легендирование
Г) Регулирование доступа

14. Какую стратегию защиты информации необходимо выбрать, если анализируются все известные угрозы и при этом существует частичное влияние на систему обработки информации (СОИ)?
А) Наступательна
я Б)
Оборонительная
В) Упреждающая
Г) Нет верного варианта ответа

15. Что относится к техническим требованиям к системе защиты информации:
А) Структурированность все компонентов
Б) Удовлетворение всем требованиям по защите
В) Оптимизация архитектуры
Г) Минимизация помех пользователям

16. Согласно организационному построению системы защиты информации к организационно-правовому обеспечению можно отнести:
А) Информационное
обеспечение Б) Техническое
обеспечение
В) Организационно-техническое
обеспечение Г) Программно-правовое
обеспечение

17. Согласно обобщенной модели процессов защиты информации Модель управления СЗИ напрямую влияет на модель:
А) Воздействия внешней среды
Б) Процессов функционирования СОИ
В) Оценки безопасности
информации Г) Воздействия
злоумышленников

18. Сложность выбора показателей, позволяющих дать адекватную оценку защищенности информации, НЕ определяется параметром:
А) Необходимостью контроля большого количества средств и объектов
защиты Б) Случайность внешних воздействий в системе обработки
информации
В) Наличием аналогов показателей, учитывающих специфику объекта информатизации и особенности ее функционирования
Г) Необходимость получения не только качественной, но и количественной оценки защищенности информации

19. Сколько существует вариантов подходов к проектированию СЗИ?
А) 2
Б)
1

В) 3
Г) Больше 3
20. Что не относится к обоснованию требований и анализу условий защиты информации:
А) формирование факторов, влияющих на защиту информации
Б) оценка защищенности информации в условиях решения выбранных задач выбранными средствами;
В) классификация технических проектных решений;
Г) определение перечня задач по защите информации, перекрывающих все потенциально

Ключ к тесту

Вариант 1	Вариант 2
1 б	1 б
2 б	2 г
3 д	3 а
4 г	4 б
5 д	5 а
6 а	6 в
7 в	7 г
8 в	8 а
9 г	9 в
10 а	10 г
11 б	11 б
12 г	12 г
13 б	13 в
14 в	14 а
15 б	15 в
16 в	16 в
17 д	17 б
18 б	18 в
19 г	19 г
20 а	20 а