Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Удмуртский государственный университет»
Институт экономики и управления
Кафедра государственной службы и управления персоналом

А.А. Мухин

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Практикум

Ижевск
2025

ISBN 978-5-4312-1289-5

УДК 34:004(075.8)
ББК 67.401.114я73-5
М925

Рекомендовано к изданию учебно-методическим советом УдГУ

Рецензенты: канд. экон. наук, доцент каф. экономики ФГБОУ ВО «Удмуртский государственный университет» **Е.В. Кутяшова,**
канд. экон. наук, зав. каф. менеджмента и права, ФГБОУ ВО «Удмуртский государственный аграрный университет» **Д.В. Кондратьев.**

Мухин А.А.

М925 Информационная безопасность : практикум / А.А. Мухин. – Ижевск : Удмуртский университет, 2025. – Электрон. (символьное) изд. (2,1 Мб). – 168 с. – Текст : электронный.

Предназначено для студентов юридических вузов, обучающихся по направлениям и специальностям «Юриспруденция», «Юриспруденция (бакалавр)», «Правоохранительная деятельность», «Судебная и прокурорская деятельность», «Правовое обеспечение национальной безопасности», «Государственное и муниципальное управление», а также для аспирантов юридических вузов, практических работников.

Соответствует актуальным требованиям Федерального государственного образовательного стандарта высшего образования.

Решение задач преследует цель закрепить теоретические знания, полученные на теоретических занятиях.

ISBN 978-5-4312-1289-5

Минимальные системные требования:
Celeron 1600 Mhz; 128 Мб RAM; WindowsXP/7/8 и выше; разрешение экрана 1024×768 или выше; программа для просмотра pdf

Мухин Алексей Арьевич
Информационная безопасность
Практикум

Подписано к использованию 11.09.2025
Объем электронного издания 2,1 Мб, тираж 10 экз
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, 4Б, каб. 021.
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru

Оглавление

ПРЕДИСЛОВИЕ

Методические рекомендации по выполнению практических заданий используется при изучении дисциплины «Основы информационной безопасности».

В методических рекомендациях рассмотрены следующие темы: общая теория безопасности, риски и угрозы в области экономической безопасности, правовые режимы обеспечения безопасности информации ограниченного доступа, угрозы в области информационной безопасности, защита конфиденциальной информации и государственной тайны, комплексная безопасность предприятия, безопасность электронных ресурсов, систем и процессов, физическая безопасность предприятия, инженерно-техническая безопасность (ИТБ) предприятия, кадровая безопасность предприятия, классификация и особенности инженерно-технических средств безопасности, взаимодействие частных и государственных институтов в сфере экономической безопасности, правовое регулирование отношений в сфере охраны государственной тайны, организационные основы и техника обеспечения безопасности банка, ответственность за правонарушения в информационной сфере.

Цели преподавания курса:

Формирование у студентов представления об информационных отношениях; о субъектах информационно-правовых отношений; правовом режиме получения, передачи, хранения и использования информации; юридических аспектах информационного обмена, информационной безопасности, ответственности в информационной сфере.

Задачи освоения дисциплины:

- определение места и роли защиты государственной тайны и информационного законодательства в современном информационном обществе;
- изучение организации в России информационно-правого обеспечения органов государственной власти, юридических и физических лиц;
- обеспечение законности и правопорядка, экономической безопасности общества, государства, личности и иных субъектов экономической деятельности;
- выработать у студентов и слушателей навыки и умения, необходимые для профессионального выполнения служебных задач.

Подготовка высококвалифицированных специалистов для работы в органах государственной власти (в том числе в правоохранительных органах) и в других сферах (юридическое обслуживание предпринимательской деятельности, управление организациями, кадровое дело, правовое образование и т. д.); обеспечивать безопасность государства, общества и личности.

Изучение основ информационной безопасности позволит обучающемуся овладеть следующими компетенциями:

Знать:

- правовые, организационные и технические основы обеспечения безопасности банка;
- основные угрозы в области обеспечения физической безопасности предприятия в сфере защиты жизни и здоровья физических лиц, обеспечения сохранности финансовых и иных материальных ценностей, а также объектов недвижимости;
- роль, место и функции системы безопасности в обеспечении защиты от внутренних и внешних угроз;
- определение понятия экономической безопасности предприятия.

Уметь:

- осуществлять внутриорганизационную деятельность кредитных организаций, направленную на создание и функционирование системы их безопасности;
- сопоставлять основные угрозы с типовыми мерами обеспечения физической защиты бизнеса;
- организовывать построение модели безопасности типового предприятия в соответствии с правилом первичности угроз по отношению к защитным мерам, а также принципом декомпозиции системы «угроза-защита»;
- определять наиболее уязвимые для угроз сферы активности бизнеса, а также угрозы, порождаемые фактом осуществления разнообразных уголовных правонарушений в сфере экономики, деловой активности, связанных с ними коррупционными рисками, рисками вовлечения в сферу деятельности криминальной среды, а также сферу теневой экономики;
- осуществлять внутриорганизационную деятельность организаций, направленную на создание и функционирование системы их безопасности;
- применять юридическую ответственность за нарушение законодательства в информационной сфере.

Владеть:

- методами обеспечения физической безопасности предприятия с применением различных типов защиты;
- навыками выявления, предупреждения и предотвращения конкретных видов преступных посягательств на интересы кредитной организации;

- принципами построения эффективной организационно-штатной структуры службы безопасности предприятия с учетом особенностей подбора и расстановки ее персонала.
- основами выявления, предупреждения и минимизации рисков угроз экономической безопасности предприятия.

ГЛАВА 1. НАЦИОНАЛЬНАЯ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Задание 1. _____ – это объективно значимые потребности личности, общества и государства в безопасности и устойчивом развитии. (вписать пропущенные два слова)

Задание 2. Технические меры обеспечения информационной безопасности представляют собой:

Выберите все правильные ответы (один или несколько)

1) создание систем для предотвращения несанкционированного доступа к информации, а также иных технических систем, обеспечивающих информационную безопасность человека, общества и государства;

2) выявление систем, технических устройств, программ, представляющих опасность вмешательства в деятельность защищенных информационных систем;

3) создание нормативной базы в информационной сфере, способной регулировать информационные отношения;

4) разработку и совершенствование средств и иных мер защиты информации и методов контроля, развитие телекоммуникационных систем и современного программного обеспечения.

Задание 3. _____ – это состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны. (вписать пропущенные два слова)

Задание 4. Выберите организационные меры обеспечения информационной безопасности:

Выберите все правильные ответы (один или несколько)

1) разработка и совершенствование средств и иных мер защиты информации и методов контроля, развитие телекоммуникационных систем и современного программного обеспечения;

2) создание системы обеспечения информационной безопасности в Российской Федерации;

3) осуществление правоприменительной деятельности органов государственной власти, направленной на предупреждение и пресечение правонарушений в информационной сфере;

4) создание нормативной базы в информационной сфере, способной регулировать информационные отношения.

Задание 5. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных:

Выберите все правильные ответы (один или несколько)

1) на реализацию права на доступ к информации;

2) на соблюдение конфиденциальности информации;

3) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования;

4) на обеспечение защиты информации от правомерного доступа.

Задание 6. К числу правовых мер, направленных на защиту информации, относятся:

Выберите все правильные ответы (один или несколько)

1) создание систем для предотвращения несанкционированного доступа к информации, а также иных технических систем, обеспечивающих информационную безопасность человека, общества и государства;

2) создание системы обеспечения информационной безопасности в Российской Федерации;

3) выявление систем, технических устройств, программ, представляющих опасность вмешательства в деятельность защищенных информационных систем;

4) создание нормативной базы в информационной сфере, способной регулировать информационные отношения.

Задание 7. К сферам обеспечения информационной безопасности относятся:

Выберите все правильные ответы (один или несколько)

1) интересы общества, состоящие в развитии демократии, создании и функционировании общественных институтов, духовном развитии, а также в формировании и поддержании общественного согласия;

2) интересы государства в политической, экономический, военной, международной сферах деятельности, в обеспечении суверенитета, территориальной целостности, общественного порядка и социальной стабильности;

3) интересы отдельных групп лиц, состоящие в развитии и функционировании общественных и культурно-идеологических институтов;

4) интересы личности в части реализации конституционных прав, включая право на доступ к информации, защиту личного пространства, чести и достоинства человека.

Задание 8. Национальная безопасность включает в себя:

Выберите все правильные ответы (один или несколько)

1) все виды безопасности, предусмотренные Конституцией Российской Федерации;

2) только оборону страны;

3) оборону страны и общественную, информационную, экологическую, экономическую;

4) оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации.

Задание 9. Выберите национальные интересы в информационной сфере, закрепленные в Доктрине информационной безопасности Российской Федерации:

Выберите все правильные ответы (один или несколько)

1) развитие отрасли информационных технологий и электронной промышленности;

2) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на защиту суверенитета РФ в информационном пространстве;

3) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры;

4) обеспечение и защита всех конституционных прав и свобод человека и гражданина.

Задание 10. Выберите виды ответственности, которые входят в систему ответственности за правонарушения в информационной сфере:

Выберите один правильный ответ

1) административная, гражданско-правовая и уголовная;

2) гражданско-правовая и уголовная;

3) дисциплинарная, гражданско-правовая и уголовная;

4) дисциплинарная, административная, гражданско-правовая и уголовная.

Задание 11. _____ – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие РФ, оборона и безопасность государства. (вписать пропущенные два слова)

ГЛАВА 2. ПОНЯТИЕ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЕ ЕЕ БЕЗОПАСНОСТИ

Задание 1. Первая законодательная формулировка понятия «информация» в России была приведена:

Выберите все правильные ответы (один или несколько)

1) в Гражданском Кодексе Российской Федерации;

2) в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации»;

3) в Конституции Российской Федерации;

4) в Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Задание 2. _____ – это сведения (сообщения, данные) независимо от формы их представления. (вписать пропущенное слово)

Задание 3. В основе информационного обмена лежит соответствующий предмет, которым является _____. (вписать пропущенное слово)

Задание 4. _____ – это совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств. (вписать пропущенные два слова)

Задание 5. Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов – это _____. (вписать пропущенное слово)

ГЛАВА 3. ИНФОРМАЦИОННЫЕ ОТНОШЕНИЯ КАК ОБЪЕКТ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ И ИХ БЕЗОПАСНОСТЬ

Задание 1. Отношения между участниками общественных отношений возникают по поводу:

Выберите все правильные ответы (один или несколько)

1) всех благ одновременно;
2) общественных благ;
3) каких-либо абстрактных благ;
4) каких-либо конкретных благ.

Задание 2. Информационные отношения в системе иных отношений охраняются уголовным законом и являются _____ уголовно-правовой охраны. (вписать пропущенное слово)

Задание 3. В наиболее упрощенном представлении под _____ преступления понимается то, на что посягает субъект преступления, чему причиняется или может быть причинен определенный вред в результате совершения преступления. (вписать пропущенное слово)

Задание 4. Для обеспечения охраны конкретного социального блага государство применяет:

Выберите все правильные ответы (один или несколько)

1) уголовно-правовое ограничение;
2) уголовно-правовой запрет;
3) гражданско-правовой запрет;
4) административно-правовой запрет.

Задание 5. _____ – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных). (вписать пропущенные два слова)

Задание 6. В.Н. Кудрявцев, указывая на общественные отношения как на объект преступления, замечает, что он охватывает собой:

Выберите все правильные ответы (один или несколько)

1) материальные формы, условия и предпосылки существования этих отношений;
2) правовую форму общественных отношений;

3) фактические общественные отношения между людьми, которые выражаются в действиях или определенном положении людей по отношению друг к другу и в обществе в целом;

4) намерения участников отношений, условия и предпосылки существования этих намерений.

ГЛАВА 4. ИНФОРМАЦИЯ КАК ПРЕДМЕТ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ

Задание 1. Преступления в информационной сфере имеют:

Выберите все правильные ответы (один или несколько)

1) один объект посягательства, который находится в одной главе УК РФ;

2) один объект посягательства, но части объекта находятся в разных главах УК РФ;

3) различные объекты посягательства, которые находятся в одной главе УК РФ;

4) различные объекты посягательства и находятся в разных главах УК РФ.

Задание 2. Угроза применения насилия при разбое связана с использованием информации о _____ возможности причинения вреда жизни или здоровью потерпевшего, которая является средством, облегчающим завладение чужим имуществом. (вписать пропущенное слово)

Задание 3. Механизмы причинения вреда общественным отношениям (объекту) через воздействие на предмет:

Выберите все правильные ответы (один или несколько)

1) различны, но не зависят от конструктивных особенностей диспозиции соответствующей статьи Особенной части УК РФ;

2) однообразны и не зависят от конструктивных особенностей диспозиции соответствующей статьи Особенной части УК РФ;

3) различны и зависят от конструктивных особенностей диспозиции соответствующей статьи Особенной части УК РФ;

4) однообразны и зависят от конструктивных особенностей диспозиции соответствующей статьи Особенной части УК РФ.

Задание 4. В теории уголовного права по признаку наличия или отсутствия предмета преступлений раньше последние делились:

Выберите все правильные ответы (один или несколько)

1) на преступления с двойным предметом;

2) на многопредметные преступления;

3) на так называемые беспредметные преступления;

4) на преступления, имеющие предмет.

Задание 5. Под _____ преступления в науке уголовного права обычно понимают предметы материального мира, при воздействии на которые причиняется вред объекту преступления. (вписать пропущенное слово)

ГЛАВА 5. УГОЛОВНАЯ ОТВЕТСТВЕННОСТЬ ЗА ПОСЯГАТЕЛЬСТВА НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Задание 1. Объективная сторона нарушения неприкосновенности частной жизни характеризуется:

Выберите один правильный ответ

1) пассивной формой поведения;
2) активной формой поведения;
3) комбинированной формой поведения;
4) дискретной формой поведения.

Задание 2. Для определения наличия или отсутствия личной или семейной тайны, необходимо исходить:

Выберите один правильный ответ

1) только из объективного критерия;
2) из объективного и субъективного критериев;
3) только из субъективного критерия;
4) только из легальной дефиниции.

Задание 3. Клеветнической информация может быть признана в случаях:

Выберите один или несколько вариантов

1) если она является ложной;
2) если она является правдивой;
3) если она порочит честь и достоинство лица или подрывает его репутацию;
4) если она только порочит честь и достоинство лица.

Задание 4. Предметом нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений является:

Выберите один правильный ответ

1) информация, получаемая или передаваемая только посредством письменной переписки;
2) только личная информация, получаемая или передаваемая посредством письменной переписки, телефонных переговоров, почтовых, телеграфных сообщений;
3) информация, получаемая или передаваемая только посредством телефонных переговоров;
4) любая информация, получаемая или передаваемая посредством письменной переписки, телефонных переговоров, почтовых, телеграфных сообщений.

Задание 5. Распространение информации, касающаяся тайны усыновления (удочерения), влечет уголовную ответственность:

Выберите один правильный ответ

1) по ст. 137 УК РФ;
2) по совокупности ст. ст. 155 и 137 УК РФ;
3) по ст. 155 УК РФ;
4) не влечет уголовной ответственности.

Задание 6. Субъект фальсификации избирательных документов или документов референдума – это _____. (вписать пропущенное слово)

Задание 7. _____ критерий личной или семейной тайны предполагает отношение самого лица к информации личного или семейного характера как нежелательной для разглашения. (вписать пропущенное слово)

Задание 8. _____ тайна может касаться отношений между супругами, проблем внутрисемейного воспитания, заболеваний членов семьи, расхождений взглядов по тем или иным вопросам между членами семьи и т. д. (вписать пропущенное слово)

Задание 9. Под неправомерным отказом в предоставлении информации понимается незаконный отказ:

Выберите один правильный ответ

1) как в письменной, так и в устной форме;
2) в основной в письменной форме, реже – в устной;
3) только в устной форме;
4) только в письменной форме.

Задание 10. _____ – это жизнедеятельность человека в сфере личных, семейных, интимных, бытовых отношений, не подлежащих контролю со стороны государства, общественных организаций, отдельных граждан. (вписать пропущенное слово)

Задание 11. Распространение заведомо ложных сведений лица о самом себе:

Выберите один правильный ответ

1) не образует состав преступления;

2) образует состав преступления, в зависимости от мнения партнеров человека;

3) образует состав преступления;

4) образует состав преступления, если сведения нанесли человеку определенный ущерб.

Задание 12. По конструкции состав клеветы является:

Выберите один правильный ответ

1) смешанным;

2) усеченным;

3) формальным;

4) материальным.

Задание 13. Отказ в предоставлении информации может выражаться:

Выберите один правильный ответ

1) как в действии, так и в бездействии;

2) только в действии;

3) в основном в бездействии, крайне редко в действии;

4) только в бездействии.

Задание 14. Состав нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений:

Выберите один правильный ответ

1) формальный;

2) материальный;

3) усеченный;

4) смешанный.

Задание 15. С субъективной стороны нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений совершается с _____ умыслом. (вписать пропущенное слово)

Задание 16. Субъектом нарушения неприкосновенности частной жизни является лицо, достигшее возраста:

Выберите один правильный ответ

1) 14 лет;
2) 18 лет;
3) 16 лет;
4) 21 года.

Задание 17. _____ – это информация о другом человеке, не соответствующая действительности. (вписать пропущенное слово)

Задание 18. По конструкции состав отказа в предоставлении гражданину информации:

Выберите один правильный ответ

1) усеченный;
2) формальный;
3) смешанный;
4) материальный.

Задание 19. Объектом нарушения неприкосновенности частной жизни являются:

Выберите один правильный ответ

1) отношения по поводу охраны неприкосновенности частной жизни;
2) информация, составляющая сведения о частной жизни лица, содержащие его личную тайну;
3) информация, составляющая сведения о частной жизни лица, содержащие его семейную тайну;
4) отношения по поводу охраны неприкосновенности частной и публичной жизни.

Задание 20. Состав плагиата по конструкции:

Выберите один правильный ответ

1) материальный;
2) усеченный;
3) смешанный;
4) формальный.

Задание 21. Предметом нарушения неприкосновенности частной жизни является:

Выберите один правильный ответ

1) отношения по поводу охраны неприкосновенности частной и публичной жизни;

2) информация, составляющая сведения о частной жизни лица, содержащие только его личную тайну;

3) отношения по поводу охраны неприкосновенности частной жизни;

4) информация, составляющая сведения о частной жизни лица, содержащие его личную или семейную тайну.

Задание 22. Объективная сторона нарушения неприкосновенности частной жизни заключается в нарушении неприкосновенности частной жизни и в соответствии с УК РФ может выражаться:

Выберите один или несколько вариантов

1) в незаконном их распространении;

2) в незаконном собирании сведений о частной жизни;

3) в незаконном их распространении в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации;

4) в их распространении в непубличном выступлении.

Задание 23. Информация, касающаяся тайны усыновления (удочерения):

Выберите один правильный ответ

1) образует предмет семейной тайны;

2) не образует предмет семейной тайны;

3) образует предмет семейной тайны, но только если раскрытие тайны произошло, пока ребенок не достиг 7-ми лет;

4) это остается на усмотрение суда.

Задание 24. К _____ правам относятся интеллектуальные права на результаты исполнительской деятельности (исполнения), на фонограммы, на сообщение в эфир или по кабелю радио- и телепередач (вещание организаций эфирного и кабельного вещания), на содержание баз данных, а также на произведения науки, литературы и искусства, впервые обнародованные после их перехода в общественное достояние. (вписать пропущенное слово)

Задание 25. Субъективная сторона нарушения неприкосновенности частной жизни характеризуется _____ умыслом. (вписать пропущенное слово)

Задание 26. _____ избирательных документов или документов референдума — это внесение ложных сведений в эти документы. (вписать пропущенное слово)

Задание 27. Субъективная сторона клеветы выражается в _____ умысле. (вписать пропущенное слово)

Задание 28. _____ – это распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. (вписать пропущенное слово)

Задание 29. Субъектом нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений является лицо, достигшее:

Выберите один правильный ответ

1) 14 лет;
2) 18 лет;
3) 21 года;
4) 16 лет.

Задание 30. _____ критерий личной или семейной тайны определяется сложившимися в обществе нравственными и моральными представлениями о том, что действительно может являться личной или семейной тайной. (вписать пропущенное слово)

Задание 31. Предметом клеветы является:

Выберите один правильный ответ

1) информация, содержащая любые сведения;

2) информация, содержащая заведомо правдивые сведения, порочащие честь и достоинство другого лица или подрывающие его репутацию;

3) информация, содержащая заведомо ложные сведения, порочащие честь и достоинство другого лица или подрывающие его репутацию;

4) информация, содержащая любые ложные сведения, порочащие честь и достоинство другого лица или подрывающие его репутацию.

Задание 32. _____ критерий личной или семейной тайны определяется сложившимися в обществе нравственными и моральными представлениями о том, что действительно может являться личной или семейной тайной. _____ являются сведения, содержащие утверждения о нарушении гражданином действующего законодательства, совершении нечестного поступка, неправильном, неэтичном поведении в личной, общественной или политической жизни, недобросовестности при осуществлении производственно-хозяйственной и предпринимательской деятельности, нарушении деловой этики или обычаев делового оборота, которые умаляют честь и достоинство гражданина или его деловую репутацию. (вписать пропущенные два слова)

Задание 33. Предоставление _____ информации – это сообщение сведений, не соответствующих действительности. (вписать пропущенные два слова)

Задание 34. Предоставление _____ информации – это ознакомление гражданина не со всеми документами и прочими информационными материалами, затрагивающими его права и свободы. (вписать пропущенное слово)

Задание 35. Объектом клеветы выступают:
Выберите один правильный ответ
1) честь, достоинство человека;
2) честь, достоинство и здоровье человека;
3) честь, достоинство человека и его репутация;
4) честь, достоинство, репутация человека и его здоровье.

Задание 36. Потерпевшим от клеветы может быть:
Выберите один правильный ответ
1) любое физическое и юридическое лицо;
2) любое физическое лицо;
3) только определенные группы физических лиц;
4) любое юридическое лицо.

Задание 37. _____ – это создание определенных условий, препятствий, чтобы воздействовать на лицо для реализации им своего конституционного права или выполнения своих служебных обязанностей, касающихся организации выборов. (вписать пропущенное слово)

Задание 38. _____ – это предоставление кандидату в депутаты любых имущественных благ, выгод или услуг имущественного характера для осуществления им определенного поведения в пользу подкупающего. (вписать пропущенное слово)

Задание 39. В конечном счете информация может быть признана личной или семейной тайной исходя из представлений _____. (вписать пропущенное слово)

Задание 40. Объективная сторона фальсификации избирательных документов, документов референдума может быть выражения:

Выберите один правильный ответ

1) только в действии;
2) только в бездействии;
3) в основном в бездействии, реже – в действии;
4) как в действии, так и в бездействии.

Задание 41. _____ – это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгодую (вписать пропущенные два слова)

Задание 42. _____ – это не подлежащая разглашению информация об операциях, счетах и вкладах своих клиентов и корреспондентов. (вписать пропущенные два слова)

ГЛАВА 6. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ГЛОБАЛИЗАЦИИ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА

Задание 1. _____ – это защищенность от внешних и внутренних угроз киберпространства. (вписать пропущенное слово)

Задание 2. Как называются процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, ориентированные на решение конкретных прикладных задач обработки информации?

Выберите все правильные ответы (один или несколько)

1) базы данных;
2) информационные системы;
3) информационные технологии;
4) информационная инфраструктура.

Задание 3. _____ – это система технических средств и организационных структур, обеспечивающих возможность выполнения задач обработки и передачи информации в рамках реализации субъективных прав и позитивных обязанностей субъектов информационной сферы. (вписать пропущенное слово)

Задание 4. _____ – это представленные в объективной форме совокупности самостоятельных материалов, систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ. (вписать пропущенное слово)

Задание 5. К числу объектов информационной безопасности могут быть отнесены:

Выберите все правильные ответы (один или несколько)

1) информация;
2) объекты информационной инфраструктуры общества;
3) интересы субъектов информационной сферы;
4) общественное регулирование.

Задание 6. Каким образом может трактоваться понятие «информационной безопасности»?

Выберите все правильные ответы (один или несколько)

1) стратегия государственного развития;
2) результат деятельности по обеспечению информационной безопасности;

3) стратегия развития национальной безопасности;

4) состояние защищенности человека, общества и государства в информационной сфере.

Задание 7. _____ – это совокупность знаний, нравственных ценностей, обычаев, традиций, стереотипов поведения. (вписать пропущенное слово)

Задание 8. К объектам идеологического противоборства относят:

Выберите все правильные ответы (один или несколько)

1) политическое сознание;
2) общественное мнение;
3) общественную психологию;
4) культурный фон.

Задание 9. Какое из следующих утверждений лучше всего описывает информационную систему?

Выберите все правильные ответы (один или несколько)

1) механизм защиты данных от несанкционированного доступа;

2) комплекс информации, хранящейся в базах данных, и технологий, обеспечивающих её обработку;

3) совокупность программного обеспечения, отвечающего за управление базами данных;

4) сеть компьютеров, связанных между собой для обмена данными.

Задание 10. _____ – это совокупность проявлений деятельности человека в сфере политики, которая существует в форме политических отношений, власти, деятельности политических институтов и политических лидеров. (вписать пропущенное слово)

Задание 11. Как называется совокупность условий и факторов, наносящих или потенциально способных нанести ущерб объектам обеспечения информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) информационная угроза;
2) риск безопасности;
3) информационная среда;
4) уязвимость системы.

Задание 12. _____ – это порядок регулирования, выраженный в многообразном комплексе правовых средств, характеризующих особое сочетание взаимодействующих между собой дозволений, запретов и позитивных обязываний, создающих особую направленность регулирования. (вписать пропущенное слово)

Задание 13. На какие виды классифицируется информационное противоборство?

Выберите все правильные ответы (один или несколько)

1) естественное;
2) идеологическое;
3) информационно-техническое;
4) внутреннее.

Задание 14. Какое из следующих утверждений лучше всего описывает информацию?

Выберите все правильные ответы (один или несколько)

1) только визуальные и аудиоматериалы;
2) только данные, хранящиеся в электронных форматах;
3) исключительно текстовые сообщения;
4) сведения, сообщения и данные независимо от формы их представления.

Задание 15. Какое из следующих утверждений лучше всего описывает оружие?

Выберите все правильные ответы (один или несколько)

1) инструменты, применяемые только в военных действиях;
2) любое средство, приспособленное и пригодное для нападения или защиты, а также совокупность таких средств;
3) комплекс устройств для самообороны в быту;
4) средства, используемые исключительно для охоты.

Задание 16. Силы обеспечения информационной безопасности Российской Федерации включают:

Выберите все правильные ответы (один или несколько)

1) Вооруженные Силы РФ;
2) граждан РФ;
3) федеральные органы государственной власти;
4) воинские формирования и органы, в которых федеральным законодательством предусмотрена военная и (или) правоохранительная служба.

ГЛАВА 7. ТЕОРЕТИЧЕСКИЕ И МЕТОДОЛОГИЧЕСКИЕ ВОПРОСЫ ОРГАНИЗАЦИОННОГО И ПРАВОВОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задание 1. К межотраслевым принципам правового обеспечения (правового регулирования) информационной безопасности относятся:

Выберите все правильные ответы (один или несколько)

1) принцип законности;
2) принцип комплексности;
3) принцип обеспечения информации;
4) принцип доступа к информации.

Задание 2. Основными источниками права в области национальной безопасности, составляющими правовую систему в Российской Федерации, являются:

Выберите все правильные ответы (один или несколько)

1) Стратегия национальной безопасности Российской Федерации;
2) Федеральный закон «О безопасности»;
3) целевые доктрины о национальной безопасности Российской Федерации;
4) международные обычаи и общепризнанные принципы и нормы международного права.

Задание 3. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

Выберите все правильные ответы (один или несколько)

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
2) установление ограничений доступа к информации только федеральными законами;
3) открытость информации;
4) установление нормативными правовыми актами преимуществ применения одних информационных технологий перед другими.

Задание 4. Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

Выберите все правильные ответы (один или несколько)

1) интеграция и взаимосвязь всех технологий;
2) достоверность информации и своевременность ее предоставления;
3) неприкосновенность частной жизни;
4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации.

Задание 5. _____ – это многоаспектная система, включающая несколько уровней коммуникационной инфраструктуры. (вписать пропущенное слово)

Задание 6. Обеспечение национальных интересов Российской Федерации осуществляется посредством реализации следующих стратегических национальных приоритетов:

Выберите все правильные ответы (один или несколько)

1) общественное сознание;
2) наука, технологии и образование;
3) экология живых систем и рациональное природопользование;
4) культура;
5) экономический рост;
6) здравоохранение.

Задание 7. К отраслевым принципам правового обеспечения (правового регулирования) информационной безопасности относятся:

Выберите все правильные ответы (один или несколько)

1) принцип баланса интересов личности, общества и государства в области обеспечения информационной безопасности;
2) принцип достоверности информации;
3) принцип технологической обусловленности;
4) принцип свободы информации.

Задание 8. _____ – это действие, направленное на достижение определенного состояния или уровня безопасности объекта в целях предотвращения утечки, хищения, утраты, искажения, подделки информации, угроз безопасности личности, общества, государств. (вписать пропущенное слово)

Задание 9. Как называется набор знаков, с помощью которых соответствующие сведения могут быть переданы от одного человека другому и восприняты им или восприняты устройствами автоматизированной обработки информации?

Выберите все правильные ответы (один или несколько)

1) информация в форме «рассылки»;
2) информация в форме «данных»;
3) информация в форме «текста»;
4) информация в форме «сообщений».

Задание 10. Единая сеть электросвязи состоит из расположенных на территории РФ сетей электросвязи следующих категорий:

Выберите все правильные ответы (один или несколько)

1) технологические сети связи;
2) сеть связи общего пользования;
3) внутренние сети связи;
4) узконаправленные сети связи;
5) выделенные сети связи.

Задание 11. К юридическим критериям обособления той или иной совокупности норм в конкретный правовой институт относятся:

Выберите все правильные ответы (один или несколько)

1) обособление норм, образующих правовой институт, в главах, разделах, частях и иных структурных единицах;
2) субъект обособления;
3) юридическое единство правовых норм;
4) полнота регулирования определенной совокупности общественных отношений.

Задание 12. Общая информационная инфраструктура состоит из следующих элементов:

Выберите все правильные ответы (один или несколько)

1) субъекты объединения;
2) сети связи и средства доступа к сетям связи;
3) информационные системы;
4) индустрия создания и развития средств информатизации и связи.

ГЛАВА 8. ОРГАНИЗАЦИОННО-ПРАВОВЫЕ ПРОБЛЕМЫ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задание 1. Соблюдение безопасности определяется как:

Выберите все правильные ответы (один или несколько)

1) понятность информации;
2) доступность информации;
3) конфиденциальность информации;
4) целостность информации;
5) идентификация информации.

Задание 2. В Законе США «Об управлении информационной безопасностью» 2002 г. информационная безопасность определяется как:

Выберите все правильные ответы (один или несколько)

1) защита от несанкционированного доступа;
2) повсеместность распространения;
3) обеспечение целостности информации;
4) обеспечение конфиденциальности.

Задание 3. _____ – это обработанная в определенном порядке совокупность документированной информации в информационных системах. (вписать пропущенные два слова)

Задание 4. Вопросы неприкосновенности частной жизни регулируются в следующих законодательных актах США:

Выберите все правильные ответы (один или несколько)

1) «О защите от преследований» 1997 г.;
2) «О полиции» 1997 г.;
3) «О судах» 1993 г.;
4) «О вещании» 1996 г.;
5) «О реабилитации правонарушителей» 1974 г.;
6) «О телекоммуникациях» 1984 г.

Задание 5. В каком году принята Конвенция о защите физических лиц при автоматизированной обработке персональных данных?

Выберите все правильные ответы (один или несколько)

1) В 1991 г.
2) В 1975 г.
3) В 1999 г.
4) В 1981 г.

ГЛАВА 9. ПРАВОВЫЕ РЕЖИМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ ОГРАНИЧЕННОГО ДОСТУПА

Задание 1. Как называется комплексный показатель, характеризующий требования, исполнение которых обеспечивает нейтрализацию определенных угроз безопасности персональных данных при их обработке в информационных системах персональных данных?

Выберите все правильные ответы (один или несколько)

1) индикатор;
2) уровень защищенности;
3) уровень обработки;
4) комплексный признак.

Задание 2. _____ информации – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. (вписать пропущенное слово)

Задание 3. _____ – это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. (вписать пропущенные два слова)

Задание 4. Как называются материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов?

Выберите все правильные ответы (один или несколько)

1) комплексы;
2) информационная среда;
3) носители сведений;
4) информационная система.

Задание 5. Тайна какого вида включает в себя как конфиденциальную информацию, представляемую в орган государственной власти, так и информацию, создаваемую в этом органе, доступ к которой временно ограничен в интересах государственного управления по решению руководителя?

Выберите все правильные ответы (один или несколько)

1) коммерческая тайна;
2) служебная тайна;
3) производственная тайна;
4) государственная тайна.

Задание 6. _____ к государственной тайне – это процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений. (вписать пропущенное слово)

Задание 7. _____ – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. (вписать пропущенные два слова)

Задание 8. При осуществлении своих прав и свобод каждый человек должен подвергаться только таким ограничениям, какие установлены законом исключительно с целью обеспечения:

Выберите все правильные ответы (один или несколько)

1) общественного контроля и общего благосостояния;
2) удовлетворения справедливых требований морали;
3) общественного порядка;
4) должного признания и уважения прав и свобод других.

Задание 9. _____ – это определенные сведения, которые должны быть защищены от несанкционированного доступа, так как распространение может нанести вред (ущерб) интересам субъектов правоотношений. (вписать пропущенное слово)

Задание 10. _____ – это любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту). (вписать пропущенные два слова)

Задание 11. Не могут относиться к служебной информации ограниченного распространения:

Выберите все правильные ответы (один или несколько)

1) сведения о чрезвычайных ситуациях;

2) описание структуры органа исполнительной власти, его функций, направлений и форм деятельности, а также его адрес;

3) сведения о деятельности организации;

4) акты законодательства, устанавливающие правовой статус государственных органов, организаций, общественных объединений.

Задание 12. _____ – это реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него. (вписать пропущенные два слова)

Задание 13. Право на информацию отнесено к разряду:

1) факультативных прав;

2) основных прав;

3) дополнительных прав;

4) специальных прав.

Задание 14. Признаками информации, в отношении которой может быть введен режим коммерческой тайны, являются:

Выберите все правильные ответы (один или несколько)

1) введение обладателем режима коммерческой тайны в отношении этих сведений;

2) ограниченный круг субъектов;

3) действительная или потенциальная коммерческая ценность в силу неизвестности этих сведений третьим лицам;

4) отсутствие свободного доступа на законном основании.

Задание 15. _____ персональных данных – это любое действие (операция) или совокупность действий (операций) персональными данными, совершаемых с использованием средств автоматизации или без использования таких средств. (вписать пропущенное слово)

ГЛАВА 10. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРАВОВОГО И ОРГАНИЗАЦИОННОГО ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задание 1. К экстремистским материалам относятся:

Выберите все правильные ответы (один или несколько)

1) любые публикации, описывающие события, признанные преступными в соответствии с приговором Нюрнбергского трибунала;

2) публикации, оправдывающие практику совершения военных или иных преступлений, направленных на частичное уничтожение какой-либо религиозной группы;

3) публикации, оправдывающие практику совершения военных или иных преступлений, направленных на полное или частичное уничтожение какой-либо этнической группы;

4) публикации, обосновывающие или оправдывающие национальное и (или) расовое превосходство.

Задание 2. К экстремистским материалам относятся:

Выберите все правильные ответы (один или несколько)

1) труды фашистской партии Италии;

2) любые сведения о преступлениях фашистской партии Италии;

3) изображения руководителей групп, организаций или движений, признанных преступными в соответствии с приговором Нюрнбергского трибунала;

4) труды руководителей национал-социалистской рабочей партии Германии.

Задание 3. Под экстремистской деятельностью понимается:

Выберите все правильные ответы (один или несколько)

1) публичное оправдание терроризма и иная террористическая деятельность;

2) возбуждение социальной, расовой, национальной или религиозной розни;

3) пропаганда исключительности, превосходства либо неполноценности человека по признаку его языковой принадлежности;

4) организация, планирование, подготовка, финансирование и реализация насильственных действий с целью устрашения населения.

Задание 4. К информации, распространение которой среди детей определенных возрастных категорий ограничено, относится информация:

Выберите все правильные ответы (один или несколько)

1) представляемая в виде изображения или описания жестокости;

2) представляемая в виде изображения или описания половых отношений между мужчиной и женщиной;

3) оправдывающая противоправное поведение;

4) содержащая бранные слова и выражения, не относящиеся к нецензурной брани.

Задание 5. _____ – это владелец сайта и (или) страницы сайта в сети Интернет, на которых размещается общедоступная информация и доступ к которым в течение суток составляет более трех тысяч пользователей сети Интернет. (вписать пропущенное слово)

Задание 6. _____ – это субъекты предоставляющие пользователям свое оборудование и технологии для хранения информации, организующие и обеспечивающие процессы обмена информацией. (вписать пропущенные два слова)

Задание 7. К информации, запрещенной для распространения среди детей, относится информация

Выберите все правильные ответы (один или несколько)

1) оправдывающая противоправное поведение;

2) отрицающая семейные ценности и формирующая неуважение к родителям и (или) другим членам семьи;

3) содержащая нецензурную брань;

4) представляемая в виде изображения или описания жестокости.

Задание 8. _____ – это предназначенная для оборота на территории РФ продукция средств массовой информации, печатная продукция, аудиовизуальная продукция на любых видах носителей, программы для ЭВМ и базы данных, а также информация, распространяемая посредством зрелищных мероприятий, посредством информационно-телекоммуникационных сетей, в том числе сети Интернет, и сетей подвижной радиотелефонной связи. (вписать пропущенные два слова)

ГЛАВА 11. ОСОБЕННОСТИ ОРГАНИЗАЦИОННО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ

Задание 1. К фундаментальным принципам обеспечения безопасности относятся:

Выберите все правильные ответы (один или несколько)

1) принцип комплексности;
2) принцип менеджмента риска;
3) принцип связей;
4) принцип служебных обязанностей и ответственности.

Задание 2. К фундаментальным принципам обеспечения безопасности относятся:

Выберите все правильные ответы (один или несколько)

1) принцип управления жизненным циклом АС;
2) принцип обязательств;
3) принцип зависимости;
4) принцип развития.

Задание 3. _____ – это все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, подотчетности, аутентичности и достоверности информации или средств ее обработки. (вписать пропущенные два слова)

Задание 4. _____ – это правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее ИТТ управлять, защищать и распределять активы, в том числе критичную информацию. (вписать пропущенные два слова)

Задание 5. _____ – это совокупность нескольких базовых стандартов и других нормативных документов с четко определенными подмножествами обязательных и факультативных возможностей, предназначенная для реализации заданной функции или группы функций. (вписать пропущенные два слова)

Задание 6. Какие выделяют группы профилей информационных систем?

Выберите все правильные ответы (один или несколько)

1) комплексные профили проектирования ИС;

2) профили, регламентирующие архитектуру ИС и ее компонентов;

3) профили единообразия;

4) профили, регламентирующие процессы проектирования, разработки, применения, сопровождения и развития ИС и их компонентов.

Задание 7. Под собственной информационной безопасностью автоматизированных систем понимается такое ее состояние, при котором обеспечивается защита:

Выберите все правильные ответы (один или несколько)

1) процессов и технологий, протекающих и реализуемых в информационной системе;

2) системы от различных физических и информационных разрушающих воздействий;

3) субъектов использования;

4) информации о самой системе.

Задание 8. К материальным активам относятся:

Выберите все правильные ответы (один или несколько)

1) здания организации;

2) базы данных;

3) средства связи и передачи данных;

4) вычислительные средства.

Задание 9. Основными функциями службы информационной безопасности являются:

Выберите все правильные ответы (один или несколько)

1) реализация функций с помощью системы аутентификации автоматизированных рабочих мест;

2) уведомление совета по безопасности о выявленных нарушениях политик безопасности и теневое копирование в архив найденных подозрительных файлов;

3) сканирование всех доступных сетевых и локальных хранилищ информации;

4) учет субъектов информационной защиты.

ГЛАВА 12. ЮРИДИЧЕСКАЯ ОТВЕТСТВЕННОСТЬ ЗА ПРАВОНАРУШЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ

Задание 1. За неисполнение или ненадлежащее исполнение работником по его вине возложенных на него трудовых обязанностей, работодатель имеет право применить следующие дисциплинарные взыскания:

Выберите все правильные ответы (один или несколько)

1) штраф;
2) замечание;
3) увольнение;
4) выговор.

Задание 2. В качестве общих признаков юридической ответственности можно выделить следующие:

Выберите все правильные ответы (один или несколько)

1) наступление неблагоприятных последствий для правонарушителя;
2) комплексный характер;
3) отсутствие взаимосвязей;
4) применение государственно-правового принуждения.

Задание 3. _____ информации – это изменение ее содержания по сравнению с той информацией, которая до совершения этого деяния была в распоряжении собственника или законного пользователя. (вписать пропущенное слово)

Задание 4. _____ – это противоправное, виновное деяние (действие или бездействие) в информационной сфере в виде неисполнения или ненадлежащего исполнения работником возложенных на него трудовых обязанностей. (вписать пропущенное слово)

Задание 5. Под нежелательными функциями подразумеваются:

Выберите все правильные ответы (один или несколько)

1) несанкционированное уничтожение компьютерной информации;
2) создание компьютерной информации;
3) блокирование компьютерной информации;
4) модификация компьютерной информации.

Задание 6. Признаками информационных преступлений являются:

Выберите все правильные ответы (один или несколько)

1) короткий срок совершения преступления;

2) проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации;

3) нарушение законных прав и свобод граждан в информационной сфере;

4) умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ.

Задание 7. _____ компьютерной информации – это невозможность ее использования при сохранности такой информации. (вписать пропущенное слово)

Задание 8. В качестве общих признаков юридической ответственности можно выделить следующие:

Выберите все правильные ответы (один или несколько)

1) зависимость;

2) регулирование нормами права;

3) наличие правонарушения;

4) комплексный характер.

Задание 9. При проведении служебной проверки должны быть полностью, объективно и всесторонне установлены:

Выберите все правильные ответы (один или несколько)

1) контакты гражданского служащего;

2) обстоятельства, послужившие основанием для письменного заявления гражданского служащего о проведении служебной проверки;

3) характер и размер вреда, причиненного гражданским служащим в результате этого проступка;

4) вина гражданского служащего.

Задание 10. При проведении служебной проверки должны быть полностью, объективно и всесторонне установлены:

Выберите все правильные ответы (один или несколько)

1) причины и условия, способствовавшие совершению гражданским служащим информационного дисциплинарного проступка;

2) история дисциплинарных взысканий лица за последние 3 года;

3) вина гражданского служащего;

4) факт совершения гражданским служащим информационного дисциплинарного проступка.

Задание 11. За неисполнение или ненадлежащее исполнение гражданским служащим по его вине возложенных на него должностных обязанностей, администрация имеет право применить следующие дисциплинарные взыскания:

Выберите все правильные ответы (один или несколько)

1) предупреждение о неполном должностном соответствии;
2) выговор;
3) замечание;
4) штраф.

Задание 12. Информационные преступления имеют ряд особенностей:

Выберите все правильные ответы (один или несколько)

1) отсутствие субъекта;
2) двойственный объект;
3) связь с информацией является не только непосредственной, но и опосредованной наличием ее материального носителя;
4) связаны с информацией.

Задание 13. _____ – это противоправные, общественно опасные виновные деяния, совершенные в информационной сфере, родовым или непосредственным объектом посягательства которых является информация, а также связанные с использованием информационных технологий, систем и информационно-телекоммуникационных сетей, причинившие существенный вред охраняемым законом правам и интересам личности, общества и государства. (вписать пропущенные два слова)

ГЛАВА 13. ИНФОРМАЦИОННОЕ ОБЩЕСТВО

Задание 1. Совокупностью всей информации, накопленной человечеством в процессе развития науки, культуры, образования и практической деятельности людей, называют _____ ресурсы. (вписать пропущенное слово)

Задание 2. Укажите основные артефакты информационного общества:
Выберите все правильные ответы (один или несколько)

1) цифровизация;
2) опыт;
3) данные;
4) интуиция;
5) процедуры;
6) знания;
7) информация.

Задание 3. В информационном обществе формируется информационное единство всей человеческой _____. (вписать пропущенное слово)

Задание 4. Развитие и внедрение компьютерной техники в различные сферы деятельности человека способствуют улучшению процесса обработки информации, а также ее накопления, переработки и предоставления пользователю. Всё это является особенностями _____. (вписать пропущенное слово)

Задание 5. В чём состоит конечная цель информатизации общества?
Выберите все правильные ответы (один или несколько)

1) обеспечить всем членам общества доступ к надежным источникам информации;
2) повысить эффективность использования человеческих и материальных ресурсов, оптимизировать производственные затраты;
3) произвести переход производства к использованию робототехники в качестве рабочей силы;
4) обеспечить информационное обслуживание, переработку огромного количества информации.

Задание 6. Соотнесите информационные революции с примерами изобретений.

Соедините элементы попарно (неверно соединенную пару можно разбить, щелкнув на крестик)

Третья революция	печатный станок
Вторая революция	телеграф
Первая революция	информационная коммуникация
Четвертая революция	летопись

Задание 7. Производство информационных товаров и услуг на базе информационных технологий – это _____. (вписать пропущенные два слова)

Задание 8. Информация, которая полно и правильно отображает существующие явления и процессы, называется _____ информацией. (вписать пропущенное слово)

Задание 9. Укажите негативные черты дигитизации общества:

Выберите все правильные ответы (один или несколько)

1) увеличение возможностей для небольшой группы людей использовать большую часть глобальных ресурсов;

2) жесткая борьба за рынок дигитальных технологий;

3) концентрация экономического развития в регионах с наибольшим развитием информационной инфраструктуры в ущерб районам, не обеспеченным современными технологиями;

4) тенденции к обострению поляризации мировой экономики;

5) нивелирование различий между людьми по уровню образованности и объему знаний.

Задание 10. _____ – процесс всемирной экономической, политической, культурной и религиозной интеграции и унификации. (вписать пропущенное слово)

Задание 11. Что такое «knowledgegap«?

Выберите все правильные ответы (один или несколько)

1) различие между людьми по уровню знаний и умений по применению информационных технологий;

2) различие между людьми по уровню образованности и объему знаний;

3) различие между людьми по доступу к информационным источникам и технологиям;

4) различие между людьми по степени устойчивости к проявлению негативных воздействий дигитизации.

Задание 12. Существует проблема отбора _____ и _____ информации. (вписать пропущенные два слова)

Задание 13. Что такое «digitaldivide»?

Выберите все правильные ответы (один или несколько)

1) Выберите один правильный ответ различие между людьми по умениям в применении информационных технологий;

2) различие между людьми по уровню образования и объему знаний;

3) различие между людьми по степени устойчивости к проявлению негативных воздействий дигитизации;

4) различие между людьми по доступу к информационным источникам и технологиям.

Задание 14. Процессом преобразования информационного содержания в словесной, графической, звуковой и прочей форме в цифровые сигналы называется _____. (вписать пропущенное слово)

Задание 15. В чём заключается информационная безопасность?

Выберите все правильные ответы (один или несколько)

1) состояние защищенности информационных ресурсов общества, в соответствии с требованиями нормативных и законодательных актов;

2) состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере;

3) защищенность информационной системы от случайного вмешательства, наносящего ущерб владельцу информации;

4) состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное искажение.

Задание 16. Что не может быть защищаемой информацией?

Выберите все правильные ответы (один или несколько)

1) информация о надвигающемся стихийном бедствии по отношению к населению, которому это стихийное бедствие угрожает;

2) информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации;

3) любая документированная информация, распространение которой может нанести ущерб ее собственнику, владельцу, пользователю или иному лицу;

4) сведения, на использование и распространение которых введены ограничения их собственником.

Задание 17. Процедурой программирования поведения человека с помощью специальных препаратов и психотехник является _____. (вписать пропущенное слово)

Задание 18. Что такое защищаемая информация?

Выберите все правильные ответы (один или несколько)

1) любая информация, которая появляется в СМИ;

2) информация, подлежащая защите согласно требованиям уголовного и административного кодекса;

3) информация – предмет собственности, подлежащий защите в соответствии с требованиями, устанавливаемыми собственником информации;

4) информация, которая подлежит защите в соответствии с требованиями правовых документов и обязательно относится к государственной тайне.

Задание 19. _____ – это использование потоков информации для оказания воздействия на формирование мнения индивида. (вписать пропущенное слово)

Задание 20. Распространением заведомо ложной информации, часто предоставляемой государством или его агентами иностранным властям или СМИ с целью оказать влияние их на мнение или политику, называется _____. (вписать пропущенное слово)

ГЛАВА 14. ИНФОРМАЦИОННО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ

Задание 1. Укажите характеристики информационной безопасности:
Выберите все правильные ответы (один или несколько)

1) актуальность;
2) рациональность;
3) доступность;
4) системность;
5) целостность;
6) иерархичность;
7) конфиденциальность.

Задание 2. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения – _____ информации. (вписать пропущенное слово)

Задание 3. Защищаемая физическим лицом информация личного характера, распространение которой может нанести моральный или материальный ущерб отдельному физическому лицу – _____ тайна. (вписать пропущенное слово)

Задание 4. Какие элементы входят в российскую классификацию информации?
Выберите все правильные ответы (один или несколько)

1) конфиденциальная информация;
2) информация для внутреннего использования;
3) открытая информация;
4) строго конфиденциальная информация.

Задание 5. Совокупностью целенаправленных действий по обеспечению безопасности данных называется _____ информации. (вписать пропущенное слово)

Задание 6. Что означает конфиденциальность информации?
Выберите все правильные ответы (один или несколько)

1) актуальность и непротиворечивость информации;
2) защищенность информации от правонарушителей и несанкционированных изменений;
3) возможность за разумное время получить требуемую информацию;
4) защиту от несанкционированного доступа к информации.

Задание 7. физическое или юридическое лицо, которое случайно совершило действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами – _____. (вписать пропущенное слово)

Задание 8. Что не является формой уязвимости информации?
Выберите все правильные ответы (один или несколько)
1) несанкционированное уничтожение носителя информации;
2) подделка информации;
3) стабилизация информации;
4) хищение носителя информации.

Задание 9. Что является нарушением статуса информации?
Выберите все правильные ответы (один или несколько)
1) удаление информации;
2) модификация информации;
3) нарушение доступности информации;
4) унификация информации.

Задание 10. Событие, возникающее как результат стечения обстоятельств, когда в силу каких-то причин используемые средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторов и нежелательного их воздействия на защищаемую информацию – _____ информации. (вписать пропущенное слово)

Задание 11. Как в общем случае называют человека, который предпринимает попытки реализации угрозы?
Выберите все правильные ответы (один или несколько)
1) крэкер;
2) взломщик;
3) хакер;
4) злоумышленник.

Задание 12. Сопоставьте последствия уязвимости информации с их определениями.

Утрата	Потеря или хищение носителя информации, уничтожение носителя информации или информации на нем, модификация или блокирование защищаемой информации
Утечка	Несанкционированное доведение защищаемой информации до неограниченного количества получателей информации
Разглашение	Неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования

Задание 13. Что называют попыткой реализации угрозы?

Выберите все правильные ответы (один или несколько)

1) атаку;
2) хакинг;
3) взлом;
4) фишинг.

Задание 14. Расположите вредоносные программы в порядке от более простых к более сложным.

Выберите все правильные ответы (один или несколько)

1) Троян;
2) Червь;
3) Вирус.

Задание 15. Перед вами два утверждения

1) Информация на жестком диске может разрушиться только вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя;
2) Вирусы для мобильных ОС являются самым быстрорастущим сегментом.

Выберите один правильный ответ

1) оба варианта верны;
2) только второй вариант верный;
3) только первый вариант верный;
4) оба варианта неверны.

Задание 16. Что такое сетевой червь?

Выберите все правильные ответы (один или несколько)

1) файл, который при запуске «заражает» другие;
2) специальная программа, способная размножаться;
3) программа для отслеживания вирусов;
4) средство для проверки дисков.

Задание 17. Компьютерная программа, реализующая полезную функцию и содержащая дополнительные скрытые функции, которые тайно используют законные полномочия инициирующего процесса в ущерб безопасности – _____. (вписать пропущенные два слова)

Задание 18. Какими отличительными особенностями обладает компьютерный вирус?

Выберите все правильные ответы (один или несколько)

1) способность к самостоятельному запуску;
2) способность к повышению помехоустойчивости операционной системы;
3) значительный объем программного кода, который позволяет вирусу ослаблять компьютерную систему без копирования самого себя;
4) способность к созданию помех в корректной работе компьютера;
5) возможность запускаться при открытии с правами администратора.

ГЛАВА 15. ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ

Задание 1. Укажите характеристики информационной безопасности:
Выберите все правильные ответы (один или несколько)

1) актуальность;
2) рациональность;
3) доступность;
4) системность;
5) целостность;
6) иерархичность;
7) конфиденциальность.

Задание 2. Актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения – _____ информации. (вписать пропущенное слово)

Задание 3. Защищаемая физическим лицом информация личного характера, распространение которой может нанести моральный или материальный ущерб отдельному физическому лицу – _____ тайна (вписать пропущенное слово).

Задание 4. Какие элементы входят в российскую классификацию информации?

Выберите все правильные ответы (один или несколько)

1) конфиденциальная информация;
2) информация для внутреннего использования;
3) открытая информация;
4) строго конфиденциальная информация.

Задание 5. Совокупностью целенаправленных действий по обеспечению безопасности данных называется _____ информации. (вписать пропущенное слово)

Задание 6. Что означает конфиденциальность информации?

Выберите все правильные ответы (один или несколько)

1) актуальность и непротиворечивость информации;
2) защищенность информации от правонарушителей и несанкционированных изменений;
3) возможность за разумное время получить требуемую информацию;
4) защиту от несанкционированного доступа к информации.

Задание 7. физическое или юридическое лицо, которое случайно совершило действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами – это _____ (вписать пропущенное слово).

Задание 8. Что не является формой уязвимости информации?

Выберите все правильные ответы (один или несколько)

1) несанкционированное уничтожение носителя информации;
2) подделка информации;
3) стабилизация информации;
4) хищение носителя информации.

Задание 9. Что является нарушением статуса информации?

Выберите все правильные ответы (один или несколько)

1) удаление информации;
2) модификация информации;
3) нарушение доступности информации;
4) унификация информации.

Задание 10. Событие, возникающее как результат стечения обстоятельств, когда в силу каких-то причин используемые средства защиты не в состоянии оказать достаточного противодействия проявлению дестабилизирующих факторов и нежелательного их воздействия на защищаемую информацию – _____ информации. (вписать пропущенное слово)

Задание 11. Как в общем случае называют человека, который предпринимает попытки реализации угрозы?

Выберите один правильный ответ

1) крэкер;
2) взломщик;
3) хакер;
4) злоумышленник.

12. Сопоставьте последствия уязвимости информации с их определениями.

Утрата	Потеря или хищение носителя информации, уничтожение носителя информации или информации на нем, модификация или блокирование защищаемой информации
Утечка	Несанкционированное доведение защищаемой информации до неограниченного количества получателей информации
Разглашение	Неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования.

Задание 13. Что называют попыткой реализации угрозы?

Выберите все правильные ответы (один или несколько)

1) атаку;
2) хакинг;
3) взлом;
4) фишинг.

Задание 14. Расположите вредоносные программы в порядке от более простых к более сложным.

Выберите все правильные ответы (один или несколько)

1) Троян;
2) Червь;
3) Вирус.

Задание 15. Перед вами два утверждения

1) Информация на жестком диске может разрушиться только вследствие действия компьютерного вируса или злого умысла вашего недоброжелателя;
2) Вирусы для мобильных ОС являются самым быстрорастущим сегментом.

Выберите один правильный ответ

1) оба варианта верны;
2) только второй вариант верный;
3) только первый вариант верный;
4) оба варианта неверны.

Задание 16. Что такое сетевой червь?

Выберите все правильные ответы (один или несколько)

1) файл, который при запуске «заражает» другие;
2) специальная программа, способная размножаться;
3) программа для отслеживания вирусов;
4) средство для проверки дисков.

Задание 17. Компьютерная программа, реализующая полезную функцию и содержащая дополнительные скрытые функции, которые тайно используют законные полномочия инициирующего процесса в ущерб безопасности – _____. (вписать пропущенные два слова)

Задание 18. Какими отличительными особенностями обладает компьютерный вирус?

Выберите все правильные ответы (один или несколько)

1) способность к самостоятельному запуску;
2) способность к повышению помехоустойчивости операционной системы;
3) значительный объем программного кода, который позволяет вирусу ослаблять компьютерную систему без копирования самого себя;
4) способность к созданию помех в корректной работе компьютера;
5) возможность запускаться при открытии с правами администратора.

ГЛАВА 16. ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ БЕЗОПАСНОСТЬ В СРЕДЕ ИНФОРМАЦИОННО-КОММУНИКАТИВНЫХ ТЕХНОЛОГИЙ

Задание 1. Укажите нехарактерные для коммуникации при помощи компьютерных сетей особенности:

Выберите все правильные ответы (один или несколько)

1) богатство эмоционального компонента общения;

2) возможность одновременного общения большого числа людей, находящихся в разных частях света и живущих в разных культурах;

3) возможность использования большей части невербальных средств коммуникации и самопрезентации;

4) повышение психологического риска в процессе общения.

Задание 2. Сопоставьте способы общения в сети Интернет с их определениями.

MMORPG	Система пересылки почтовых сообщений между абонентами
E-mail	Разновидность онлайновых ролевых игр, позволяющая множеству людей одновременно играть в изменяющемся виртуальном мире через Интернет
Форум	Средство общения пользователей по сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение
Чат	Организация обмена информацией и общения между большим количеством собеседников, которым небезынтересна тема обсуждения, которая и является причиной концентрации этих людей в одном месте для вынесения её на всеобщее обсуждение

Задание 3. Что является достоинством блога?

Выберите все правильные ответы (один или несколько)

1) высокая продуктивность общения;

2) мгновенный обмен сообщениями;

3) иллюзия востребованности;

4) возможность самореализации.

Задание 4. Социальной структурой, состоящей из группы узлов, которыми являются социальные объекты, и связей между ними, называется _____.

Выберите пропущенное слово:

1) ресурс;
2) блог;
3) влог;
4) социальная сеть.

Задание 5. С помощью какого средства происходит замена невербального общения в киберпространстве?

Выберите все правильные ответы (один или несколько)

1) смайл;
2) раскрытие персональных данных;
3) аватар;
4) акроним.

Задание 6. Кто следит за соблюдением правил ресурса?

Выберите все правильные ответы (один или несколько)

1) декодер;
2) пользователь;
3) администратор;
4) подписчик.

Задание 7. Что относят к основной психологической особенности интернет-общения?

Выберите все правильные ответы (один или несколько)

1) анонимность;
2) машинальность общения;
3) стремление к типичному, нормативному поведению;
4) долговременность.

Задание 8. Каких смайлов не бывает?

Выберите все правильные ответы (один или несколько)

1) текстовых;
2) структурных;
3) анимированных;
4) стикеров.

Задание 9. Место куда попадает заблокированный пользователь – _____. (вписать пропущенное слово).

Задание 10. Что понимают под определением информационной культуры?

Выберите все правильные ответы (один или несколько)

1) способ жизнедеятельности человека в информационном обществе, как составляющая процесса формирования культуры человечества;

2) открытые и скрытые целенаправленные информационные воздействия систем друг на друга с целью получения определенного выигрыша в материальной сфере;

3) состояние хранимых, обрабатываемых и передаваемых данных, при котором невозможно их случайное или преднамеренное получение, изменение или уничтожение;

4) необходимость получения информации, требуемой для решения конкретных задач, стоящих перед пользователем.

Задание 11. Кто является автором понятия «нетикет»?

Выберите все правильные ответы (один или несколько)

1) М. Семаго;
2) К. Янг;
3) В. Ши;
4) В.И. Загвязинский.

Задание 12. Соотнесите понятия с их определениями.

Этика	Наука, изучающая мораль, нравственность как форму общественного сознания и как вид общественных отношений
Этикет	Правила хорошего тона, принятые в социальной группе
Нетикет	Правила поведения, общения в сети Интернет
Компьютерная этика	Нормы поведения в сетевой среде

Задание 13. Какое правило включено в сетевой этикет?

Выберите все правильные ответы (один или несколько)

1) «помните, что вы говорите с человеком, уважайте время и возможности других»;

2) «в сети не существует рамок, ограничивающих поведение, нет цензуры и правил»;

3) «в сети действуют другие нормы и правила, чем в реальной жизни»;

4) «умейте отстаивать свою позицию, иначе собеседники не будут вас уважать».

Задание 14. На каких уровнях, в зависимости от субъекта-носителя, можно рассматривать информационную культуру?

Выберите все правильные ответы (один или несколько)

1) личности;
2) отдельных групп;
3) нации;
4) общества;
5) государства.

Задание 15. Информационное поведение отражает _____ личности как познающего субъекта.

Выберите пропущенное слово:

1) умение;
2) активность;
3) деятельность;
4) стремление.

Задание 16.Термин «интернет-зависимость» ввёл _____

Выберите пропущенное слово:

1) В. Ши;
2) К. Янг;
3) А. Голдберг;
4) И. Подласый.

Задание 17. Размещение в сети сообщений, направленных на разжигание ссоры – _____

Выберите пропущенное слово:

1) флейм;
2) спам;
3) кряк;
4) флуд.

Задание 18. Различные формы негативного поведения лиц, сфера нравственных пороков, отступление от принципов, норм морали и права – показатели _____ поведения. (вписать пропущенное слово)

ГЛАВА 17. ВВЕДЕНИЕ В ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

Задание 1. Какие IT-системы строятся на технологиях одного производителя?

Выберите все правильные ответы (один или несколько)

1) проектные;
2) реверсивные;
3) модульные;
4) закрытые.

Задание 2. Как соотносятся понятия «функциональная безопасность» и «информационная безопасность»?

Выберите все правильные ответы (один или несколько)

1) понятие «информационная безопасность» шире;
2) понятие «функциональная безопасность» шире;
3) они равноценны;
4) их нельзя сопоставить.

Задание 3. Наличие скрытых каналов в IT-системе:

Выберите все правильные ответы (один или несколько)

1) свидетельствует о возможности диверсии;
2) свидетельствует о правонарушениях;
3) свидетельствует о низкой эффективности защиты;
4) является неизбежным.

Задание 4. Как называют проверку подлинности?

Выберите все правильные ответы (один или несколько)

1) контроль;
2) идентификация;
3) конфиденциальность;
4) аутентификация.

Задание 5. Как называется изменение персональных данных с целью затруднения установления соответствия между конкретным человеком и конкретными данными?

Выберите все правильные ответы (один или несколько)

1) дигитализация;
2) анонимизация;
3) обобщение;
4) логинизация.

Задание 6. Что в информационной безопасности понимается под риском?

Выберите все правильные ответы (один или несколько)

1) возможность отклонения от плана;
2) вероятность реализации конкретной угрозы;
3) вероятность реализации конкретной угрозы и возможные потери от этой угрозы;
4) наличие конкретных угроз.

Задание 7. Как называется нападающий, который имеет мало знаний и использует для атаки готовые средства (программы, скрипты и т. д.)?

Выберите все правильные ответы (один или несколько)

1) скрипт-кидди;
2) саботажник;
3) хакер;
4) скрипт-профи.

Задание 8. Одним из важнейших принципов компьютерной криминалистики является:

Выберите все правильные ответы (один или несколько)

1) работа только с копиями;
2) решение в пользу более крупной IT-системы;
3) рассмотрение всех участников под их IP-адресами;
4) стремление расследовать происшествие в максимально сжатые сроки.

Задание 9. Что является примером четких правил, выполнение которых можно проконтролировать?

Выберите все правильные ответы (один или несколько)

1) пользователи должны принимать все возможные меры для защиты своих паролей;
2) все пользователи должны выполнять указания системного администратора;
3) все пользователи обязаны создавать только надежные пароли;
4) все пользовательские пароли должны меняться 1 раз в 3 месяца.

ГЛАВА 18. УГРОЗЫ

Задание 1. Запись данных в некоторую область без предварительной проверки, подходят ли эти данные этой области, может вести к этой ошибке:

Выберите все правильные ответы (один или несколько)

1) вредоносная запись;
2) системный сбой;
3) перезапись исходных данных;
4) переполнение буфера.

Задание 2. Что не является компонентом компьютерного вируса?

Выберите все правильные ответы (один или несколько)

1) идентификатор вируса;
2) инфицирующая часть;
3) драйвер;
4) деструктивная часть.

Задание 3. Какой анализ позволяет обнаружить даже неизвестные вирусы?

Выберите все правильные ответы (один или несколько)

1) проектный;
2) эвристический;
3) логистический;
4) системный.

Задание 4. Методы борьбы с компьютерными вирусами делятся:

Выберите все правильные ответы (один или несколько)

1) на активные и проактивные;
2) на основные и второстепенные;
3) на активные и пассивные;
4) на превентивные и активные.

Задание 5. Чем компьютерные вирусы первого поколения отличаются от вирусов второго поколения?

Выберите все правильные ответы (один или несколько)

1) только деструктивное воздействие;
2) воздействуют только на системные файлы;
3) простое уничтожение с помощью антивирусной программы;
4) не требуют помещения зараженных файлов в карантин.

Задание 6. Почему компьютерные вирусы появились не с появлением компьютеров, а позднее?

Выберите все правильные ответы (один или несколько)

1) никому ранее не приходило в голову вредить чужим компьютерам;
2) компьютерные вирусы еще не были изобретены;
3) не было специалистов;
4) все программное обеспечение сначала устанавливалось и тестировалось на сервере.

Задание 7. В чем главная угроза макровируса?

Выберите все правильные ответы (один или несколько)

1) он сразу рассылается всем контактам;
2) он находится в неисполняемом файле, а не в программе;
3) он поражает весь компьютер;
4) он не может быть уничтожен антивирусной программой.

Задание 8. Чем черви отличаются от компьютерных вирусов?

Выберите все правильные ответы (один или несколько)

1) не могут рассылать себя;
2) последовательно заражают все файлы компьютера;
3) не выявляются антивирусными программами;
4) для проникновения используют дыры и ошибки.

Задание 9. Что не используется для борьбы с троянскими конями?

Выберите все правильные ответы (один или несколько)

1) помещение полученных по незащищенным каналам файлов в карантин минимум на 5 дней;
2) использование программ с цифровыми подписями;
3) инспекция кода программы на изменения;
4) принцип минимальных прав.

Задание 10. Что необходимо для деактивации бот-сети?

Выберите все правильные ответы (один или несколько)

1) выслать всем ботам команду деактивации;
2) удалить центральный сервер;
3) провестидезинтеграциюсети;
4) запустить в бот-сеть опасный вирус.

Задание 11. Что не относится к опасностям применения мобильных систем?

Выберите все правильные ответы (один или несколько)

1) ориентация пользователей на удобство работы, а не на безопасность;
2) вероятность потери или кражи;
3) частые подключения с различным уровнем доверия;
4) возможность самовоспламенения аккумулятора.

ГЛАВА 19. ПРОБЛЕМЫ БЕЗОПАСНОСТИ ИНТЕРНЕТ-ПРОТОКОЛОВ

Задание 1. В протоколе TCP порт является:
Выберите все правильные ответы (один или несколько)
1) номером уровня модели TCP/IP;
2) адресом произвольной длины;
3) 16-битным адресом;
4) 32-битным адресом.

Задание 2. IP-адреса являются _____. (вписать пропущенное слово)

Задание 3. Задачи какого уровня модели ISO/OSI выполняет протокол IP?
Выберите все правильные ответы (один или несколько)
1) сигнального;
2) уровня приложений;
3) сетевого;
4) транспортного.

Задание 4. Для динамического назначения IP-адреса используется протокол _____. (вписать пропущенное слово)

Задание 5. Задачу замены локального IP-адреса глобальным при отправке пакетов от компьютера из внутренней сети в интернет выполняет _____. (вписать пропущенное слово)

Задание 6. Что является существенным недостатком протокола IP?
Выберите все правильные ответы (один или несколько)
1) медленная работа;
2) отсутствие шифрования заголовка и данных;
3) отсутствие сообщений об ошибках;
4) частые сбои.

Задание 7. Почему зачастую в роутерах настраивается игнорирование пакетов с активированными SourceRouting-опциями?
Выберите все правильные ответы (один или несколько)
1) эти опции устарели;
2) злоумышленник может прописать свой адрес в качестве обязательного узла, через который должен идти пакет;
3) в новых версиях протокола они не используются;
4) их использование замедляет работу.

Задание 8. Зачем отправителя пакетов могут принуждать провести фрагментацию пакетов?

Выберите все правильные ответы (один или несколько)

1) чтобы вызвать загрузку сети;
2) чтобы увеличить скорость передачи;
3) чтобы получить контроль над компьютером отправителя;
4) чтобы увеличить вероятность потери пакета.

Задание 9. Почему в IPv6 злоумышленнику нет необходимости сканировать все адресное пространство?

Выберите все правильные ответы (один или несколько)

1) идентификаторы интерфейса, как правило, генерируются по некоторому образцу;
2) злоумышленник подкупает сотрудника;
3) злоумышленник видит по адресу, в какой области сканировать;
4) злоумышленник быстро сокращает пространство для сканирования.

Задание 10. Что содержит Reverse-зона базы DNS-сервера?

Выберите все правильные ответы (один или несколько)

1) соответствие между MAC-адресом и IP-адресом;
2) соответствие между IP-адресом и доменным именем;
3) соответствие между доменным именем и IP-адресом;
4) соответствие между IP-адресом и MAC-адресом.

Задание 11. Какое средство поможет предотвратить DNS-спуфинг?

Выберите все правильные ответы (один или несколько)

1) шифрование;
2) ручное управление средствами контроля;
3) использование биометрии;
4) двойной поиск в базе данных.

Задание 12. Как называется файловая система, которая позволяет получить доступ к файлам, которые управляются на сервере?

Выберите все правильные ответы (один или несколько)

1) PPP;
2) FTP;
3) NFC;
4) NFS.

Задание 13. Для скрытия информации об отправителе электронного письма могут использоваться:

Выберите все правильные ответы (один или несколько)

1) серверы;
2) узлы-посредники;
3) ремейлеры;
4) антивирусные программы.

Задание 14. Как называется демонстрация жертве специально подготовленного сайта вместо истинного?

Выберите все правильные ответы (один или несколько)

1) сервер-снуфинг;
2) веб-сервер-спуфинг;
3) подделка сеанса;
4) сеанс-пруфинг.

Задание 15. Какая угроза безопасности может возникать из-за использования SSL через браузер?

Выберите все правильные ответы (один или несколько)

1) браузер некоторое время сохраняет данные в открытом виде;
2) злоумышленник может воздействовать на отображение браузером информации о защищенности;
3) SSL имеет ключ недостаточной для современных реалий длины;
4) SSL является достаточно простым алгоритмом.

ГЛАВА 20. ПОСТРОЕНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ

Задание 1. Каждый доступ изначально запрещен и может быть разрешен только явным выражением этого. Как называется данный принцип?

Выберите все правильные ответы (один или несколько)

1) принцип запрещения;
2) принцип назначения;
3) принцип контроля;
4) принцип разрешения.

Задание 2. Методы и механизмы, используемые при проектировании системы, должны быть доступны, чтобы надежность системы не зависела от сохранения этих механизмов в тайне. Как называется данный принцип?

Выберите все правильные ответы (один или несколько)

1) принцип гласности;
2) принцип открытости;
3) принцип открытой конструкции;
4) принцип минимальных прав.

Задание 3. Для определения потребности в защите следует использовать оборот:

Выберите все правильные ответы (один или несколько)

1) сколько будет достаточно для…
2) что будет, если…
3) когда будет возможно, что…
4) почему может быть, что…

Задание 4. Какой метод часто используется при анализе угроз?

Выберите все правильные ответы (один или несколько)

1) сопоставление рисков;
2) сравнение потерь;
3) «дерево угроз»;
4) «цепь опасностей».

Задание 5. Для определения вероятности, с которой тот или иной риск может превратиться в реальную атаку, необходимо сравнить:

Выберите все правильные ответы (один или несколько)

1) расходы, которые понесет нападающий на проведение атаки, и выгоды, которые он получит;
2) выгоды нападающего и третьей стороны;
3) потери и приобретения нападающего;
4) потери «жертвы» и выгоды нападающего.

Задание 6. Что относится к вторичному ущербу?

Выберите все правильные ответы (один или несколько)

1) потери из-за остановки производства;
2) ущерб имиджу;
3) расходы на восстановление;
4) выплаты сотрудникам.

Задание 7. Если программное обеспечение в процессе разработки в состоянии защитить себя и обрабатываемую информацию от врага или хотя бы в какой-то степени противостоять атакам, то реализована парадигма:

Выберите все правильные ответы (один или несколько)

1) безопасность в производстве;
2) безопасность в разработке;
3) непрерывная конфиденциальность;
4) безопасность программного обеспечения.

Задание 8. Что не относится к этапам проведения теста?

Выберите все правильные ответы (один или несколько)

1) попытка определения операционной системы, ее версии, браузера и т. п.;
2) определение открытых портов и служб;
3) попытка поджога серверного помещения;
4) поиск свободной информации об объекте.

Задание 9. В чем суть концепции «черного ящика»?

Выберите все правильные ответы (один или несколько)

1) враг не имеет абсолютно никакой информации о системе;
2) враг не может оценить риски;
3) враг имеет только легкодоступную информацию о системе;
4) враг не может подкупить сотрудников атакуемой системы.

Задание 10. Что не относится к типичным тестам на атаку?

Выберите все правильные ответы (один или несколько)

1) атаки на использование известных слабых мест в программном обеспечении;

2) атаки на встраивание поддельных пакетов данных;

3) атаки на угадывание и перебор паролей;

4) атаки на систему энергоснабжения.

ГЛАВА 21. КРИТЕРИИ ОЦЕНКИ

Задание 1. В системе критериев TCSEC системы делятся на _____. (вписать пропущенные два слова)

Задание 2. Один из главных пунктов критики системы TCSEC:

Выберите все правильные ответы (один или несколько)

1) ориентация на централизованные системы;
2) ориентация на открытые системы;
3) расплывчатость требований;
4) низкий уровень защиты.

Задание 3. Какому уровню защиты соответствует ступень B в системе критериев TCSEC?

Выберите все правильные ответы (один или несколько)

1) имеется формализованное доказательство характеристик безопасности;
2) защита определяется системой;
3) система вообще не обеспечивает безопасность;
4) защита определяется пользователем.

Задание 4. Как часто называют критерии TCSEC?

Выберите все правильные ответы (один или несколько)

1) «оранжевая книга»;
2) «красный альбом»;
3) «белый список»;
4) «зеленый том».

Задание 5. В системе критериев ITSEC системы классифицируются на _____. (вписать пропущенные два слова)

Задание 6. Если сертифицированный продукт был обновлен, то сертификат:

Выберите все правильные ответы (один или несколько)

1) продлевается на неопределенный срок;
2) продлевается на срок до следующего обновления;
3) должен быть получен вновь;
4) продлевается или должен быть получен вновь в зависимости от решения производителя.

Задание 7. Что не может выступать в качестве объекта оценивания с помощью каталогов критериев?

Выберите все правильные ответы (один или несколько)

1) межсетевой экран;
2) криптосистема, операционная система;
3) система кондиционирования воздуха на рабочем месте;
4) компьютер с периферией и программным обеспечением.

Задание 8. Какая концепция вводится в системе оценивания Common-Criteria?

Выберите все правильные ответы (один или несколько)

1) профиль защиты;
2) цепочка защиты;
3) уровень защиты;
4) стена защиты.

Задание 9. Что позволяет уменьшить использование критериев оценки систем и их элементов?

Выберите все правильные ответы (один или несколько)

1) издержки;
2) длительность разработки;
3) цены;
4) неопределенность на рынке.

ГЛАВА 22. МОДЕЛИ БЕЗОПАСНОСТИ

Задание 1. Наличие модели безопасности позволяет:

Выберите все правильные ответы (один или несколько)

1) ускорить сборку и настройку;

2) добиться более высокой ступени при классификации по системам критериев;

3) упростить работу сотрудников;

4) снизить издержки реализации.

Задание 2. В системе может возникнуть ситуация, когда действия отдельных пользователей недостаточно дифференцированы и контролируемы. Из-за чего это может произойти?

Выберите все правильные ответы (один или несколько)

1) из-за слишком детального моделирования субъектов;

2) из-за слишком детального моделирования объектов;

3) из-за укрупненного моделирования субъектов;

4) из-за укрупненного моделирования объектов.

Задание 3. Чем объясняется распространение практики выдачи универсальных прав?

Выберите все правильные ответы (один или несколько)

1)такие права хорошо поддерживаются большинством операционных систем;

2) такие права гарантируют, что пользователи получат необходимый им доступ;

3) такие права наиболее эффективны;

4) такие права более понятны пользователям.

Задание 4. При использовании универсальных прав:

Выберите все правильные ответы (один или несколько)

1) объекты получают слишком большие права;

2) субъекты получают недостаточно прав;

3) объекты получают недостаточно прав;

4) субъекты получают слишком большие права.

Задание 5. Матричная модель в целом может быть охарактеризована как _____. (вписать пропущенное слово)

Задание 6. На какие две группы делятся матрицы доступа?

Выберите все правильные ответы (один или несколько)

1) подробные и схематические;
2) двухмерные и многомерные;
3) плоские и объемные;
4) статические и динамические.

Задание 7. Как называется запрет одновременного участия в разных ролях без принципиального запрета участия в этих ролях?

Выберите все правильные ответы (один или несколько)

1) статическое разделение задач;
2) принцип «уволься в одном месте – работай в другом»;
3) динамическое разделение задач;
4) принцип одной роли.

Задание 8. Для чего была разработана модель «Китайская стена»?

1) для разделения функций;
2) для предотвращения использования инсайдерской информации при консультировании;
3) для полной изоляции системы от окружающего мира;
4) для надежной защиты китайского бизнеса.

Задание 9. Что является главной целью модели Белла – Лападулы?

Выберите все правильные ответы (один или несколько)

1) информационные потоки защищены от злоумышленников;
2) информационные потоки полностью контролируются руководством;
3) информационные потоки в крайнем случае идут снизу вверх или возникают в пределах одного класса безопасности;
4) информационные потоки начинаются и заканчиваются в пределах одного класса безопасности.

Задание 10. В чем суть проблемы «слепой записи» в модели Белла – Лападулы?

Выберите все правильные ответы (один или несколько)

1) сотрудник не может убедиться, сохранился ли файл;
2) сотрудник может сделать запись, но не может прочитать сделанные им изменения;
3) сотрудник не может проконтролировать маршрут записи;
4) сотрудник не может создать резервную копию.

ГЛАВА 23. ТЕХНОЛОГИИ РАБОТЫ С КЛЮЧАМИ

Задание 1. В большинстве систем задача хранение ключей возлагается:

Выберите все правильные ответы (один или несколько)

1) на пользователей;
2) на системного администратора;
3) на директора;
4) на сотрудников службы охраны.

Задание 2. В чем особенность недетерминистских генераторов случайных чисел?

Выберите все правильные ответы (один или несколько)

1) используется программная имитация бросания монеты;
2) используются задаваемые пользователем параметры;
3) используются параметры внешних процессов;
4) ни один ответ не подходит.

Задание 3. Почему при большом числе участников неэффективна схема, при которой каждый участник договаривается с каждым о ключе?

Выберите все правильные ответы (один или несколько)

1) велик риск, что новый участник захватит роль доверенного элемента;
2) необходимо очень большое количество ключей;
3) велик риск, что злоумышленник перехватит все ключи;
4) необходимо время для подключения новых участников.

Задание 4. Чем реже меняется ключ, тем _____ он должен быть. (вписать пропущенное слово)

Задание 5. Что необходимо для повышения безопасности при обмене ключами?

Выберите все правильные ответы (один или несколько)

1) минимизировать количество передаваемых сообщений, необходимое для успешного обмена ключами;
2) сделать канал абсолютно защищенным;
3) уменьшить длину канала между участниками;
4) сократить интервал времени при обмене сообщениями.

Задание 6. Могут ли асимметричные протоколы обмена ключами использоваться без центрального сервера?

Выберите все правильные ответы (один или несколько)

1) нет, не могут;
2) могут только при использовании надежного криптоалгоритма;
3) да, могут;
4) могут только при использовании защищенных каналов.

Задание 7. Для использования симметричного алгоритма обмена ключами необходимо наличие:

Выберите все правильные ответы (один или несколько)

1) абсолютно защищенного канала;
2) доверительного сервера для аутентификации и распределения ключей;
3) защищенной электронно-цифровой подписи;
4) доверительного сервера для аутентификации и распределения ключей и защищенной электронно-цифровой подписи.

Задание 8. Почему в протоколах обмена ключами следует избегать многократного шифрования?

Выберите все правильные ответы (один или несколько)

1) есть риск, что сообщение не будет расшифровано;
2) есть риск, что злоумышленник перехватит сообщение;
3) повысятся требования к квалификации пользователей;
4) увеличатся издержки.

ГЛАВА 24. АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ЗНАНИЯ

Задание 1. Что не относится к методам аутентификации, основанным на знании?

Выберите все правильные ответы (один или несколько)

1) пароль;
2) одноразовый пароль;
3) отпечаток пальца;
4) «вызов – ответ».

Задание 2. Как в современных системах обеспечивается надежность хранения паролей на сервере?

Выберите все правильные ответы (один или несколько)

1) хранится не сам пароль, а значение хеш-функции, вычисленное на его основе;
2) ни один ответ не подходит;
3) пароли хранятся в абсолютно защищенной области памяти;
4) пароль шифруется с помощью DES-алгоритма.

Задание 3. Что нельзя использовать в пароле?

Выберите все правильные ответы (один или несколько)

1) цифры;
2) свою фамилию;
3) специальные символы;
4) заглавные буквы.

Задание 4. Выберите удачный вариант создать надежный и при этом запоминающийся пароль.

Выберите все правильные ответы (один или несколько)

1) использовать имена родственников;
2) выучить предложение или стихотворение и задать пароль по первым буквам слов;
3) использовать свой номер телефона;
4) использовать свою дату рождения.

Задание 5. Почему использование одноразовых паролей повышает безопасность?

Выберите все правильные ответы (один или несколько)

1) они генерируются обоими участниками;

2) они используются только один раз, поэтому перехват пароля ничего не дает злоумышленнику;

3) они генерируются по случайным алгоритмам;

4) ничего из перечисленного не подходит.

Задание 6. Почему вызовы лучше передавать в зашифрованном виде?

Выберите все правильные ответы (один или несколько)

1) вызовы могут дать злоумышленнику информацию о количестве участников и интенсивности коммуникации;

2) злоумышленник может формировать свои ответы и сравнивать их с теми, которые передаются по сети;

3) чем меньше информации получает злоумышленник, тем лучше;

4) ничего из перечисленного не подходит.

Задание 7. За счет чего метод «вызов – ответ» обеспечивает безопасность?

Выберите все правильные ответы (один или несколько)

1) злоумышленник не понимает смысл ответов;

2) конкретная пара «вызов – ответ» используется сейчас и будет повторена очень нескоро;

3) злоумышленник не успевает перехватить ответы;

4) между вызовом и ответом нет никакой связи.

ГЛАВА 25. АУТЕНТИФИКАЦИЯ НА ОСНОВЕ ОБЛАДАНИЯ ПРЕДМЕТОМ

Задание 1. Почему на смарт-картах используются симметричные методы шифрования?

Выберите все правильные ответы (один или несколько)

1) потому что они быстрее работают;
2) так как им нужно меньше памяти, и они быстрее работают;
3) так они становятся более простыми в использовании;
4) потому что им нужно меньше памяти.

Задание 2. Зачем EEPROM смарт-карты покрывается металлической пленкой?

Выберите все правильные ответы (один или несколько)

1) пленка является частью электрической цепи;
2) пленка закрывает EEPROM от ионизирующего излучения;
3) для красоты;
4) нет правильного ответа.

Задание 3. Почему внутренние шины смарт-карт не выводятся наружу?

Выберите все правильные ответы (один или несколько)

1) чтобы их не мог прослушать злоумышленник;
2) чтобы скрыть секретную технологию производства;
3) чтобы защитить их от повреждения;
4) ничего из перечисленного не подходит.

Задание 4. Нужна ли аутентификация системы перед смарт-картой?

Выберите все правильные ответы (один или несколько)

1) нет, аутентификация не нужна;
2) а, так как это является дополнительной проверкой, что пользователь – не злоумышленник;
3) да, так как пользователь должен быть уверен, что подключился к нужной ему системе, в которой данные будут защищены;
4) в некоторых системах аутентификация перед смарт-картой не нужна, а в некоторых нужна.

Задание 5 Какие функции выполняет TCG-чип?

Выберите все правильные ответы (один или несколько)

1) функции ключа;
2) функции смарт-карты;
3) функции постоянной памяти;
4) функции сканера.

Задание 6. Целью TCG-платформы является обеспечение безопасной _____. (вписать пропущенное слово)

Задание 7. Для чего используются физически неклонируемые функции?
Выберите все правильные ответы (один или несколько)

1) для шифрования данных;
2) для безопасной передачи данных;
3) для безопасного хранения данных;
4) для аутентификации и идентификации.

Задание 8. Какие 2 фазы различают при использовании физически неклонируемой функции?
Выберите все правильные ответы (один или несколько)

1) фаза отправки и фаза получения;
2) фаза приема и фаза передачи;
3) фаза обучения и фаза проверки;
4) фаза воздействия и фаза отклика.

Задание 9. Требование воспроизводимости результата применительно к физически неклонируемым функциям означает:

1) ничего из перечисленного не подходит;
2) при повторном вводе аргумента ответ повторится;
3) работа функции может быть описана математически;
4) проверяющий может воспроизвести функцию на компьютере и получить тот же результат.

Задание 10. Хорошим примером физически неклонируемой функции является:
Выберите все правильные ответы (один или несколько)

1) кирпич;
2) ствол дерева;
3) веревка;
4) оптическая линза с внутренними отражателями.

Задание 11. Сильная физически неклонируемая функция:
Выберите все правильные ответы (один или несколько)

1) копируема и предсказуема;
2) копируема и непредсказуема;
3) некопируема и непредсказуема;
4) некопируема и предсказуема.

ГЛАВА 26. БИОМЕТРИЧЕСКАЯ АУТЕНТИФИКАЦИЯ

Задание 1. С ростом количества учитываемых характеристик доля неверных отклонений:

Выберите все правильные ответы (один или несколько)

1) растет;
2) не меняется;
3) уменьшается;
4) нет связи между величинами.

Задание 2. Биометрическая характеристика у разных людей должна отличаться. Как называется это требование?

Выберите все правильные ответы (один или несколько)

1) дифференцированность;
2) различность;
3) уникальность;
4) однозначность.

Задание 3. Для использования биометрической характеристики необходимо, чтобы люди были согласны с ее использованием. Как называется это требование?

Выберите все правильные ответы (один или несколько)

1) консенсус;
2) толерантность;
3) приемлемость;
4) согласие.

Задание 4. Какое требование не выполняют длина и форма усов как биометрические характеристики?

Выберите все правильные ответы (один или несколько)

1) универсальность;
2) конфиденциальность;
3) количественная описываемость;
4) ничего из перечисленного не подходит.

Задание 5. В чем заключается основная проблема биометрических методов?

Выберите все правильные ответы (один или несколько)

1) сложно проводить поиск по большой базе данных;
2) ничего из перечисленного не подходит;
3) сложно решить, соответствуют ли считанные данные образцу;
4) сложно установить соответствие между данными и человеком.

Задание 6. Считывание биометрической характеристики должно обеспечиваться с необходимой точностью. Как называется это требование?

Выберите все правильные ответы (один или несколько)

1) считываемость;
2) эффективность;
3) точность;
4) тщательность.

Задание 7. С чем связан один из главных рисков, возникающих при использовании биометрических методов?

Выберите все правильные ответы (один или несколько)

1) с необходимостью демонстрировать характеристику в идеальном виде (например, вымыть руки);
2) с необходимостью закрывать те части тела, биометрические характеристики которых используются для аутентификации;
3) с неизменяемостью характеристик;
4) с необходимостью непосредственного контакта с электрическими приборами (датчиками).

Задание 8. Если сопоставить парольные и биометрические методы по уровню совпадения полученных данных с записанным образцом:

Выберите все правильные ответы (один или несколько)

1) то в парольных методах совпадение всегда 100 %, в биометрических – всегда меньше 100 %;
2) то обе группы методов основаны на 100 % совпадении;
3) то в парольных методах совпадение всегда меньше 100 %, в биометрических – всегда 100 %;
4) то обе группы методов основаны на совпадении меньше 100 %.

ГЛАВА 27. ОСОБЕННОСТИ АУТЕНТИФИКАЦИИ В РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Задание 1. Как в Blockchain блоки связываются между собой?
Выберите все правильные ответы (один или несколько)

1) каждый следующий блок содержит хеш предыдущего;
2) выход предыдущего блока является входом следующего;
3) за счет майнинга;
4) все блоки шифруются одним ключом.

Задание 2. Какую важную проблему позволяет решить технология Blockchain?
Выберите все правильные ответы (один или несколько)

1) большая протяженность линий;
2) подкуп сотрудников;
3) отсутствие доверительного центрального звена и доверительной инфраструктуры;
4) ничего из перечисленного не подходит.

Задание 3. Может ли в блокчейне возникнуть ветвление?
Выберите все правильные ответы (один или несколько)

1) да;
2) нет;
3) да, но крайне редко;
4) да, но временно.

Задание 4. Создание нового блока в блокчейне называется _____. (вписать пропущенное слово)

Задание 5. На чем основана безопасность блокчейна?
Выберите все правильные ответы (один или несколько)

1) ни один участник не знает хеш-функции;
2) участники не знают друг друга;
3) ни один участник не может собрать больше половины вычислительной мощности сети;
4) ни один участник не знает ключа.

Задание 6. Если получатель биткойнов хочет потратить сумму поступления, то он должен:

Выберите все правильные ответы (один или несколько)

1) доказать, что обладает частным ключом, который относится к хешированному публичному ключу;

2) должен обратиться к центральному звену для подтверждения операции;

3) предъявить документ, удостоверяющий личность;

4) продемонстрировать цепочку, которая дала ему данную сумму.

ГЛАВА 28. ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Задание 1. Как называется раздел математики, изучающий методы извлечения зашифрованной информации?

Выберите все правильные ответы (один или несколько)

1) криптология;
2) дешифровка;
3) криптография;
4) криптоанализ.

Задание 2. В чем заключается частотный анализ шифротекста?

Выберите все правильные ответы (один или несколько)

1) в разложении сигнала по частотам;
2) в периодическом анализе шифротекста;
3) в анализе частоты, с которой в тексте встречается та или иная буква;
4) ничего из перечисленного не подходит.

Задание 3. Если в шифре Цезаря отказаться от алфавитного порядка в нижнем алфавите, то количество комбинаций составит _____. (вставить пропущенное число)

Задание 4. Чему равно количество комбинаций в шифре перестановки с длиной блока *n*?

Выберите все правильные ответы (один или несколько)

1) $10n$
2) $(n-1)!$
3) n^3
4) $n!$

Задание 5. Если перехвачено сообщение, зашифрованное шифром перестановки, то бессмысленно проводить:

Выберите все правильные ответы (один или несколько)

1) дифференциальный криптоанализ;
2) подбор открытого текста;
3) частотный анализ;
4) подбор ключа.

Задание 6. Что можно использовать для вскрытия шифра «сцитала»?

Выберите все правильные ответы (один или несколько)

1) пирамиду;
2) конус;
3) шар;
4) цилиндр.

Задание 7. Что может быть использовано в качестве шифровального устройства в шифре «сцитала»?

Выберите все правильные ответы (один или несколько)

1) копье;
2) спичка;
3) запястье;
4) ствол дерева.

Задание 8. Что является существенным недостатком диска Энея?

Выберите все правильные ответы (один или несколько)

1) малое количество вариантов ключа;
2) тяжесть зашифрованного сообщения;
3) малая стойкость шифра;
4) отправка ключа вместе с посланием.

Задание 9. Почему в квадрате Полибия каждая буква шифруется двумя буквами?

Выберите все правильные ответы (один или несколько)

1) чтобы обезопасить передачу сообщения;
2) чтобы злоумышленник не знал, какая из этих букв истинная;
3) потому что эти 2 буквы представляют собой координаты буквы открытого текста;
4) для повышения криптографической стойкости.

Задание 10. Какую дополнительную защиту дает использование «магического квадрата», а не простой таблицы с номерами букв?

Выберите все правильные ответы (один или несколько)

1) увеличивается количество комбинаций;
2) усложняется работа злоумышленника;
3) нет возможности провести частотный анализ;
4) дополнительной защиты нет.

Задание 11. Как выглядит шифротекст, полученный с помощью шифра Аве Мария?

Выберите все правильные ответы (один или несколько)

1) последовательность цифр;
2) последовательность спецсимволов;
3) хаотическая последовательность букв;
4) связный текст.

Задание 12. Кто предложил усовершенствовать использование таблицы Тритемия за счет использования ключа-пароля?

Выберите все правильные ответы (один или несколько)

1) Чемберлен;
2) Прокофьев;
3) Степанов;
4) Белазо.

Задание 13. Если при шифровании с помощью шифра Кардано после 4 поворотов решетки остались незашифрованные буквы, то следует:

Выберите все правильные ответы (один или несколько)

1) снять решетку и вписывать буквы в свободные поля;
2) послать зашифрованную часть с предупреждением, что продолжение сообщения будет выслано позже;
3) переместить решетку на свободное поле и повторить процедуру;
4) вращать решетку далее, пока не зашифруется все сообщение.

Задание 14. В чем заключается сложность при использовании шифра Ришелье?

Выберите все правильные ответы (один или несколько)

1) сложно придумать связный текст, в который вписываются буквы секретного сообщения;
2) у получателя должна быть такая же решетка;
3) необходимо производить сложные вычисления;
4) расшифровка может длиться много дней.

Задание 15. В чем заключается суть гибридного шифрования?

Выберите все правильные ответы (один или несколько)

1) сообщение несколько раз шифруется разными алгоритмами;
2) ключ шифруется с помощью асимметричного метода, а сообщение – с помощью симметричного;
3) используется комбинация не менее трех различных алгоритмов;
4) ключ шифруется с помощью симметричного метода, а сообщение – с помощью асимметричного.

Задание 16. В чем заключается суть асимметричного шифрования?

Выберите все правильные ответы (один или несколько)

1) одна сторона имеет большее влияние на коммуникацию, чем другая;
2) сообщения могут идти только в одну сторону;
3) существуют два ключа – открытый для шифрования и секретный для расшифровывания;
4) ничего из перечисленного не подходит.

Задание 17. Асимметричные методы шифрования уступают симметричным методам тем, что они:

Выберите все правильные ответы (один или несколько)

1) являются менее стойкими;
2) требуют более высокой квалификации персонала;
3) работают медленнее;
4) подходят лишь для ограниченного числа символов.

Задание 18. Если противник может зашифровать избранный открытый текст и посмотреть результат шифрования, то атака называется:

Выберите все правильные ответы (один или несколько)

1) атака с подсказкой;
2) атака с частичным знанием;
3) атака-диверсия;
4) атака на основе подобранного открытого текста.

Задание 19. Как называется метод вскрытия шифра, в котором последовательно пробуются разные варианты ключа?

Выберите все правильные ответы (один или несколько)

1) последовательный доступ;
2) полный перебор;
3) последовательный взлом;
4) угадывание.

Задание 20. При анализе стойкости шифра исходят из некоторых допущений. Определите неверное.

Выберите все правильные ответы (один или несколько)

1) хранение ключа абсолютно безопасно;
2) противник имеет доступ к шифротексту;
3) обмен ключами абсолютно безопасен;
4) противник не знает способ шифрования.

ГЛАВА 29. СОВРЕМЕННЫЕ КРИПТОГРАФИЧЕСКИЕ АЛГОРИТМЫ

Задание 1. В чем заключается основной недостаток режима электронной шифровальной книги?

Выберите все правильные ответы (один или несколько)

1) противник может воспользоваться полным перебором;
2) пространство ключей очень маленькое;
3) одни и те же блоки открытого текста шифруются в одни и те же блоки шифротекста;
4) шифрование занимает много времени.

Задание 2. Какую операцию означает символ ⊕?

Выберите все правильные ответы (один или несколько)

1) исключающее «или»;
2) двоичное умножение;
3) логическое «или»;
4) двоичное сложение.

Задание 3. Какую особенность имеют синхронные поточные шифры?

Выберите все правильные ответы (один или несколько)

1) шифрование сообщения происходит практически мгновенно;
2) работа шифровальщика и дешифратора должна идти одновременно;
3) поток ключей рассчитывается независимо от открытого текста и шифротекста;
4) ничего из перечисленного не подходит.

Задание 4. Чем является регистр сдвига?

Выберите все правильные ответы (один или несколько)

1) основой для криптоалгоритма;
2) генератором псевдослучайных чисел;
3) генератор псевдопростых чисел;
4) ничего из перечисленного не подходит.

Задание 5. Единственный шифр с идеальной стойкостью:

Выберите все правильные ответы (один или несколько)

1) простой числовой алгоритм Хо Ши Мина;
2) метод одноразовых блокнотов Вернама;
3) DES-алгоритм многоразовых списков;
4) шифр Риббентропа единообразных таблиц.

Задание 6. Какой шифр считается идеально стойким?

Выберите все правильные ответы (один или несколько)

1) у которого только что изобретен алгоритм;
2) у которого вероятностное распределение при шифровании двух различных текстов одинаково;
3) у которого пространство ключей соответствует безопасному до 2040 г.;
4) у которого пространство ключей бесконечно.

Задание 7. Как называется рассеивание статистических особенностей открытого текста по широкому диапазону статистических характеристик шифротекста?

Выберите все правильные ответы (один или несколько)

1) разброс;
2) выброс;
3) диффузия;
4) дисперсия.

Задание 8. Как называется максимальное усложнение статистической взаимосвязи между шифротекстом и ключом?

Выберите все правильные ответы (один или несколько)

1) запутывание;
2) дисперсия;
3) конвергенция;
4) конфузия.

Задание 9. На чем основана надежность RSA-алгоритма?

Выберите все правильные ответы (один или несколько)

1) на сложности решения дифференциальных уравнений;
2) на третьем законе Евклида;
3) на сложности разложения больших чисел на простые множители;
4) на недоказуемости теоремы Ферма.

ГЛАВА 30. ЭЛЕКТРОННАЯ ЦИФРОВАЯ ПОДПИСЬ

Задание 1. В чем заключается основной принцип работы межсетевого экрана?

Выберите все правильные ответы (один или несколько)

1) любые данные пересекают границу сети только с разрешения администратора;

2) частная и открытая системы не должны связываться друг с другом;

3) все данные шифруются;

4) любой поток данных изнутри наружу или снаружи внутрь должен проходить через экран.

Задание 2. Что не входит в задачи межсетевого экрана?

Выберите все правильные ответы (один или несколько)

1) ограничение доступа;

2) подписывание документов с помощью ЭЦП;

3) протоколирование;

4) аутентификация.

Задание 3. Чем отличаются динамические пакетные фильтры отличаются?

Выберите все правильные ответы (один или несколько)

1) скорость фильтрации зависит от объема передаваемых данных;

2) правила фильтрации можно быстро изменять;

3) фильтрация зависит от пакетов, которые были проанализированы ранее;

4) правила фильтрации меняются в зависимости от времени суток.

Задание 4. На основе какого устройства можно реализовать пакетный фильтр?

Выберите все правильные ответы (один или несколько)

1) на основе МФУ;

2) на основе роутера;

3) на основе монитора;

4) на основе смартфона.

Задание 5. С каким уровнем модели ISO/OSI работают пакетные фильтры?

Выберите все правильные ответы (один или несколько)

1) с сетевым уровнем;
2) с транспортным уровнем;
3) с уровнем приложений;
4) ни с одним из указанных выше.

Задание 6. В чем недостаток использования контрольной суммы как средства защиты?

Выберите все правильные ответы (один или несколько)

1) она идет в незашифрованном виде;
2) она часто вызывает сбой;
3) она может быть пересчитана нападающим;
4) она даст верный результат при потере четного количества бит.

Задание 7. Если данные для транспортировки через сегмент сети помещаются в своего рода «конверт», интерпретация которого происходит только в пункте назначения, то это называется:

Выберите все правильные ответы (один или несколько)

1) туннелирование;
2) пропечатывание;
3) конвертирование;
4) конвертация.

Задание 8. Как называется инфраструктура, в которой компоненты частной сети связываются между собой с помощью публичной сети, причем возникает впечатление, что вся сеть используется только собственником?

Выберите все правильные ответы (один или несколько)

1) виртуальная частная сеть;
2) публично-частная сеть;
3) распределенная сеть;
4) открытая сеть.

Задание 9. Из каких двух частей состоит протокол TLS?

Выберите все правильные ответы (один или несколько)

1) из протокола записи и протокола рукопожатия;
2) из протокола записи и протокола считывания;
3) из протокола записи и протокола идентификации;
4) из протокола аутентификации и протокола авторизации.

Задание 10. Как называется защищенное расширение DNS?
Выберите все правильные ответы (один или несколько)

1) DNS Ultra Edition;
2) DNS Super;
3) DNS+;
4) DNSSEC.

ГЛАВА 31. БЕЗОПАСНОСТЬ СЕТЕЙ

Задание 1. Какой алгоритм не нужен для применения электронной цифровой подписи?

Выберите все правильные ответы (один или несколько)

1) алгоритм восстановления ключа;
2) алгоритм подписывания;
3) алгоритм создания ключа;
4) алгоритм проверки.

Задание 2. Почему в одноразовой подписи Лемпорта–Диффи ключ может использоваться только один раз?

Выберите все правильные ответы (один или несколько)

1) поскольку она действует ограниченное время;
2) поскольку он характеризуется низкой стойкостью;
3) поскольку вся подпись используется в первом же сообщении;
4) потому что половина ключа в явном виде содержится в первом же подписанном сообщении.

Задание 3. Как алгоритм шифрования RSA превращается в RSA-подпись?

Выберите все правильные ответы (один или несколько)

1) шифрование приравнивается к подписыванию;
2) отправитель подписывает документ, «расшифровывая» его своим секретным ключом, а получатель для проверки «зашифровывает» документ публичным ключом;
3) отправитель подписывает документ, «расшифровывая» его публичным ключом, а получатель для проверки «зашифровывает» документ секретным ключом;
4) алгоритм шифрования RSA дополняется DES-алгоритмом.

Задание 4. Как называется криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле? Она включает в себя алгоритм шифрования и алгоритм цифровой подписи и лежит основе бывших стандартов электронной цифровой подписи в США (DSA) и России (ГОСТ Р 34.10-94)?

Выберите все правильные ответы (один или несколько)

1) алгоритм Рабина;
2) алгоритм Эль–Гамаля;
3) одноразовая подпись Лемпорта–Диффи;
4) подпись RSA.

ГЛАВА 32. БЕЗОПАСНОСТЬ МОБИЛЬНОЙ И БЕСПРОВОДНОЙ СВЯЗИ

Задание 1. Почему в сети GSM идентификация идет по временному, а не по постоянному идентификатору?

Выберите все правильные ответы (один или несколько)

1) что можно было участвовать в системе анонимно;
2) это механизм защиты от сохранения профиля передвижений абонента;
3) постоянный идентификатор зашит в телефоне, опасно передавать его по незащищенному каналу;
4) ничего из перечисленного не подходит.

Задание 2. Как создается секретный ключ для шифрования разговора?

Выберите все правильные ответы (один или несколько)

1) генерируется сим-картой и передается аутентификационному центру;
2) генерируется базовой станцией и передается сим-карте и аутентификационному центру;
3) генерируется аутентификационным центром и передается сим-карте;
4) одновременно генерируется сим-картой и аутентификационным центром.

Задание 3. Для аутентификации типа «вызов – ответ» и для шифрования разговора аутентификационный центр генерирует:

Выберите все правильные ответы (один или несколько)

1) пароль;
2) аутентификационный триплет;
3) случайное число;
4) уникальный аутентификатор.

Задание 4. Как соотносятся GSM и GPRS?

Выберите все правильные ответы (один или несколько)

1) GPRS работает за счет параллельного использования нескольких GSM-каналов;
2) GSM является следующим шагом в развитии GPRS;
3) GPRS является следующим шагом в развитии GSM;
4) GSM работает за счет использования нескольких GPRS-каналов.

Задание 5. Что является важным в отношении информационной безопасности преимуществом UMTS по сравнению с GSM?

Выберите все правильные ответы (один или несколько)

1) двухсторонняя аутентификация;
2) парольная аутентификация;
3) двухфакторная аутентификация;
4) аутентификация «вызов – ответ».

Задание 6. Что является платой за бесшовность при переходе из сети в сеть в рамках SAE/LTE?

Выберите все правильные ответы (один или несколько)

1) низкая скорость;
2) слабая аутентификация;
3) большие издержки;
4) отсутствие антивирусной защиты.

Задание 7. Что не относится к уязвимостям сетей 5G и «интернета вещей»?

Выберите все правильные ответы (один или несколько)

1) значительное увеличение возможного вреда;
2) рост опасности DDoS-атак;
3) слабая аутентификация;
4) существенное увеличение поверхности атаки.

Задание 8. Как называется объединение до восьми участников по Bluetooth?

Выберите все правильные ответы (один или несколько)

1) микросеть;
2) пикосеть;
3) наносеть;
4) нейросеть.

Задание 9. Для чего в сетях ZigBee нужен координатор?

Выберите все правильные ответы (один или несколько)

1) он принимает и удаляет пользователей;
2) он выступает в роли доверительного центра;
3) он управляет коммуникацией;
4) ничего из перечисленного не подходит.

ГЛАВА 33. ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ

Задание 1. Как называются приборы, которые должны обнаружить угрозу и проинформировать ответственных лиц?

Выберите все правильные ответы (один или несколько)

1) датчики;
2) извещатели;
3) сирены;
4) информаторы.

Задание 2. Виброакустические каналы – это распространение сигналов:

Выберите все правильные ответы (один или несколько)

1) в воде;
2) в проводах;
3) в строительных конструкциях и инженерных коммуникациях;
4) в воздухе.

Задание 3. Что не влияет на эффективность обнаружения через оптический канал?

Выберите все правильные ответы (один или несколько)

1) скорость движения объекта;
2) количество соседних объектов;
3) яркость объекта;
4) угловые размеры объекта.

Задание 4. Что не относится к методам защиты от утечки по оптическому каналу?

Выберите все правильные ответы (один или несколько)

1) структурное скрытие;
2) пространственное скрытие;
3) временное скрытие;
4) линейное скрытие.

Задание 5. Что не относится к особенностям радиоэлектронной разведки?

Выберите все правильные ответы (один или несколько)

1) работа в непосредственном контакте с объектом наблюдения;
2) малая уязвимость;
3) охват больших пространств;
4) получение информации в режиме реального времени.

Задание 6. Как называется добывание информации о признаках объектов, проявляющихся в их собственном электромагнитном излучении?

Выберите все правильные ответы (один или несколько)

1) радиолокационная разведка;
2) радиоразведка;
3) радиотепловая разведка;
4) радиотехническая разведка.

ГЛАВА 34. ПРАВОВЫЕ ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задание 1. Какая иерархия существует в подчиненности нормативно-правовых актов?

Выберите все правильные ответы (один или несколько)

1) Указы президента, Конституция, федеральные законы, ведомственные акты;
2) Конституция, федеральные законы, указы президента, ведомственные акты;
3) Конституция, указы президента, федеральные законы, ведомственные акты;
4) Федеральные законы, указы президента, Конституция, ведомственные акты.

Задание 2. Как называется возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного характера?

Выберите все правильные ответы (один или несколько)

1) секретность личных данных;
2) ничего из перечисленного не подходит;
3) неразглашение персональных данных;
4) неприкосновенность частной жизни.

Задание 3. Право каждого гражданина искать, получать, передавать, производить и распространять информацию закреплено:

Выберите все правильные ответы (один или несколько)

1) в Конституции;
2) в федеральном законе;
3) в кодексе;
4) в указе президента.

Задание 4. Могут ли персональные данные человека быть выложены в открытом доступе?

Выберите все правильные ответы (один или несколько)

1) да, если субъект дал согласие на размещение своих персональных данных в общедоступном источнике персональных данных;
2) да, если субъект не работает в МВД;
3) да;
4) нет.

Задание 5. Что не может требовать субъект персональных данных от оператора?

Выберите все правильные ответы (один или несколько)

1) видеозаписи обработки данных;
2) сроки обработки и сроки хранения;
3) применяемые способы обработки;
4) правовые основания и цели обработки.

Задание 6. К какой информации доступ не может быть ограничен?

Выберите все правильные ответы (один или несколько)

1) к персональным данным чиновников;
2) к данным о состоянии окружающей среды;
3) к нормативным правовым актам;
4) к информации о деятельности государственных органов.

Задание 7. Что не относится к принципам использования ЭЦП?

Выберите все правильные ответы (один или несколько)

1) право использовать любую технологию связи для передачи ЭЦП;
2) право использовать ЭЦП любого вида;
3) ежедневный контроль корректности ключа;
4) недопустимость признания ЭЦП и документа недействительными только на основании того, что отсутствует собственноручная подпись.

Задание 8. Что не относится к сведениям конфиденциального характера?

Выберите все правильные ответы (один или несколько)

1) государственная тайна;
2) коммерческая тайна;
3) врачебная тайна;
4) нотариальная тайна.

ГЛАВА 35. УПРАВЛЕНИЕ IT-ПРОЕКТОМ КАК ЭФФЕКТИВНЫЙ СПОСОБ ОРГАНИЗАЦИИ ДЕЙСТВИЙ ПО ПОВЫШЕНИЮ УРОВНЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Задание 1. Почему решения в области информационной безопасности можно рассматривать как проекты?

Выберите все правильные ответы (один или несколько)

1) потому что решаемая задача уникальна;
2) потому что есть заданный бюджет;
3) потому что есть заданная цель;
4) потому что отсутствуют кадровые ограничения.

Задание 2. По отношениям между заказчиком и исполнителем проекты делятся:

Выберите все правильные ответы (один или несколько)

1) на свободные и фиксированные;
2) на внутренние и внешние;
3) на добровольные и обязательные;
4) на договорные и номенклатурные.

Задание 3. Выполняя роль модератора, менеджер проекта должен:

Выберите все правильные ответы (один или несколько)

1) быть примером для сотрудников, регулировать конфликты и т. д.;
2) руководить связями команды проекта с остальными сотрудниками;
3) ничего из перечисленного не подходит;
4) направлять беседы при обсуждениях.

Задание 4. Деление проекта на задания не может происходить:

Выберите все правильные ответы (один или несколько)

1) по географическому признаку;
2) на основе компонентов продукта;
3) на основе этапов реализации;
4) на основе структурных единиц.

ГЛАВА 36. ОСНОВНЫЕ ОПРЕДЕЛЕНИЯ

Задание 1. _____ – это гарантирует, что данные не были изменены, подменены или уничтожены в результате злонамеренных действий или случайностей. (вписать пропущенные два слова)

Задание 2. К угрозам информационной безопасности со стороны человеческого фактора не относятся:

Выберите все правильные ответы (один или несколько)

1) низкая квалификация работников;
2) действия уволенных или недовольных сотрудников;
3) анализаторы протоколов;
4) халатность.

Задание 3. Цели защиты информации:

Выберите все правильные ответы (один или несколько)

1) целостность данных;
2) доступность данных;
3) конфиденциальность данных;
4) все ответы верны.

Задание 4. К техническим средствам обеспечения информационной безопасности и защиты информации относятся:

Выберите все правильные ответы (один или несколько)

1) резервирование особо важных компьютерных подсистем;
2) недопущение ведения важных работ одним человеком;
3) защита авторских прав программистов;
4) все ответы верны.

Задание 5. К техническим угрозам информационной безопасности не относятся:

Выберите все правильные ответы (один или несколько)

1) «черви»;
2) промышленный шпионаж;
3) «троянские кони»;
4) ошибки в программном обеспечении;
5) компьютерные вирусы;
6) сетевые атаки, в том числе DoS- и DDoS-атаки.

ГЛАВА 37. ПРАВОВЫЕ АСПЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЫ ИНФОРМАЦИИ

Задание 1. Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» запрещается распространение информации, которая направлена:

Выберите все правильные ответы (один или несколько)

1) на разжигание религиозной ненависти;
2) на пропаганду войны;
3) на разжигание национальной вражды;
4) на разжигание расовой ненависти;
5) все ответы верны.

Задание 2. Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» не может быть ограничен доступ:

Выберите все правильные ответы (один или несколько)

1) к персональным данным граждан (физических лиц);
2) к информации о состоянии окружающей среды;
3) к информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств;
4) все ответы верны.

Задание 3. Согласно Федеральному закону «О безопасности» правовую основу обеспечения безопасности составляют, в частности:

Выберите все правильные ответы (один или несколько)

1) международные договоры Российской Федерации;
2) общепризнанные принципы и нормы международного права;
3) конституция;
4) все ответы верны.

Задание 4. Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» защита информации есть принятие мер, направленных:

Выберите все правильные ответы (один или несколько)

1) на соблюдение конфиденциальности информации ограниченного доступа;
2) на реализацию права на доступ к информации;
3) на предотвращение неправомерного доступа, уничтожения, модифицирования, копирования, распространения и иных неправомерных действий в отношении информации;
4) все ответы верны.

Задание 5. Национальными интересами РФ, согласно Доктрине информационной безопасности Российской Федерации, являются:

Выберите все правильные ответы (один или несколько)

1) все ответы верны;

2) защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации;

3) борьба с распространением информации о способах разработки, изготовления и использования наркотических средств, психотропных веществ;

4) развитие информационных технологий и электронной промышленности.

Задание 6. Конституция РФ содержит следующие нормы:

Выберите все правильные ответы (один или несколько)

1) законы и иные правовые акты не должны противоречить Конституции;

2) конституция имеет высшую юридическую силу, прямое действие и применяется на всей территории Российской Федерации;

3) нормы международного права и международные договоры РФ являются частью ее правовой системы; если международным договором РФ установлены иные правила, чем предусмотренные законом, то применяются правила международного договора;

4) все ответы верны.

Задание 7. Конституция РФ гарантирует следующие права и свободы:

Выберите все правильные ответы (один или несколько)

1) свободу мысли и слова;

2) право собираться мирно, без оружия, проводить собрания, митинги и демонстрации, шествия и пикетирование;

3) свободу массовой информации;

4) все ответы верны.

Задание 8. Международный пакт о гражданских и политических правах признаёт в качестве неотъемлемых прав человека:

Выберите все правильные ответы (один или несколько)

1) право на свободу мысли, совести и религии;

2) право на пропаганду расовой ненависти;

3) право на пропаганду религиозной ненависти;

4) право на пропаганду национальной ненависти;

5) право на мирные собрания.

ГЛАВА 38. МАТЕРИАЛЫ К ПРАКТИЧЕСКИМ ЗАНЯТИЯМ: ЭЛЕМЕНТЫ ТЕОРИИ ЧИСЕЛ

Задание 1. Разложение составного целого числа z на простые множители _____. (вписать пропущенное слово)

Задание 2. Наука, объединяющая в себе криптографию и криптоанализ _____. (вписать пропущенное слово)

Задание 3. Обеспечением скрытности передачи информации занимается:
Выберите все правильные ответы (один или несколько)

1) маркировка;
2) дешифрование;
3) стеганография;
4) криптоанализ.

Задание 4. Числа a и c называются мультипликативно обратными по модулю m, если:
Выберите все правильные ответы (один или несколько)

1) $a / c \equiv 1 (\mathrm{mod}\ 1 \cdot m)$;
2) $a \cdot c \equiv 1 (\mathrm{mod}\ m)$;
3) $a / c \equiv 1 / (\mathrm{mod}\ m)$;
4) $a \cdot c \equiv 1 (\mathrm{mod}\ 1/m)$.

Задание 5. Основной криптографический метод защиты информации, обеспечивающий ее конфиденциальность и аутентичность _____. (вписать пропущенное слово)

ГЛАВА 39. СЕТЕВОЕ ВЗАИМОДЕЙСТВИЕ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ СОВРЕМЕННОГО ОБЩЕСТВА

Задание 1. Что из перечисленного является преимуществом использования беспроводной сети?

Выберите все правильные ответы (один или несколько)

1) нет необходимости в кабелях;
2) более высокая скорость, чем в проводных сетях;
3) более безопасные, чем проводные сети;
4) ничего из вышеперечисленного.

Задание 2. Что такое VPN?

Выберите все правильные ответы (один или несколько)

1) безопасный способ доступа к частной сети через Интернет;
2) разновидность компьютерного вируса;
3) тип сетевого протокола;
4) тип сетевого кабеля.

Задание 3. Каковы несколько советов по эффективному налаживанию связей?

Выберите все правильные ответы (один или несколько)

1) внимательно слушать и задавать вдумчивые вопросы;
2) профессионально одеваться и приносить резюме;
3) избегать зрительного контакта и говорить тихо;
4) немедленно попроситься на работу.

Задание 4. Что из приведенного ниже является примером невербальной коммуникации в социальном взаимодействии?

Выберите все правильные ответы (один или несколько)

1) выражение лица;
2) говорящий;
3) написание;
4) отправка текстовых сообщений.

Задание 5. Каковы этические соображения, связанные с созданием сетей?

Выберите все правильные ответы (один или несколько)

1) конфиденциальность, безопасность и интеллектуальная собственность;
2) эффективность, стоимость и скорость;
3) качество, количество и скорость;
4) бренд, дизайн и качество.

Задание 6. Как нетворкинг может помочь людям найти работу и продвинуться по карьерной лестнице?

Выберите все правильные ответы (один или несколько)

1) путем установления контактов между отдельными лицами и потенциальными работодателями;

2) путем предоставления доступа к спискам вакансий;

3) помогая отдельным лицам развивать новые навыки;

4) путем предоставления доступа к бесплатному образованию.

Задание 7. Какая из перечисленных ниже топологий сети является распространенной?

Выберите все правильные ответы (один или несколько)

1) звезда;

2) квадрат;

3) треугольник;

4) круг.

Задание 8. Что такое двухфакторная аутентификация и как она помогает повысить безопасность в социальных сетях?

Выберите все правильные ответы (один или несколько)

1) функция безопасности, требующая от пользователей ввода пароля и кода, отправленного на их телефон или электронную почту;

2) функция безопасности, требующая от пользователей ввода пароля и секретного вопроса для доступа к этой учетной записи;

3) функция безопасности, которая шифрует все данные, которыми делятся на платформах социальных сетей;

4) функция безопасности, которая охватывает все входящие сообщения и отфильтровывает потенциальную угрозу.

Задание 9. Что такое «сеть» в технических системах?

Выберите все правильные ответы (один или несколько)

1) группа взаимосвязанных устройств, которые могут взаимодействовать друг с другом;

2) группа компьютеров, которые не подключены друг к другу;

3) устройство, используемое для подключения к интернету;

4) тип программного обеспечения, используемого для защиты компьютеров от вредоносных программ.

Задание 10. Что такое сетевая безопасность?

Выберите все правильные ответы (один или несколько)

1) обеспечение того, чтобы только авторизованные пользователи могли получить доступ к сети;
2) защита компьютера от вирусов;
3) настройка беспроводной сети;
4) соединение нескольких компьютеров вместе.

Задание 11. Каковы основные типы сетей?

Выберите все правильные ответы (один или несколько)

1) LAN, WAN и MAN;
2) беспроводные, проводные и гибридные;
3) государственные, частные и гибридные;
4) VPN, VLAN и VPLS.

Задание 12. Для чего нужен маршрутизатор в сети?

Выберите все правильные ответы (один или несколько)

1) для фильтрации и направления сетевого трафика;
2) для беспроводного подключения устройств;
3) для обеспечения питанием устройств в сети;
4) для шифрования сетевых данных.

Задание 13. В чем разница между сетями локальной сети и WAN?

Выберите все правильные ответы (один или несколько)

1) сети LAN используются для небольших географических районов, в то время как сети WAN используются для больших географических районов;
2) сети локальной сети являются проводными, в то время как сети глобальной сети являются беспроводными;
3) сети LAN используются для личного пользования, в то время как сети WAN используются для делового использования;
4) локальные сети более безопасны, чем сети WAN.

Задание 14. Что из перечисленного не является фактором, влияющим на социальное взаимодействие?

Выберите все правильные ответы (один или несколько)

1) физическая среда;
2) культура;
3) возраст;
4) гендер.

Задание 15. Что такое социальное взаимодействие?
Выберите все правильные ответы (один или несколько)

1) процесс общения и обмена информацией с другими;
2) процесс вовлечения в уединенную деятельность;
3) процесс избегания контактов с другими людьми;
4) процесс вовлечения в соревновательную деятельность.

ГЛАВА 40. СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ КАК ОСНОВНАЯ УГРОЗА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

Задание 1. Как проявляется воздействие социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) в использовании технологий для улучшения социальной коммуникации;

2) в использовании психологии и манипуляций для обмана отдельных лиц;

3) в использовании платформ социальных сетей для влияния на поведение;

4) в использовании искусственного интеллекта для автоматизации социальных взаимодействий.

Задание 2. Как организации могут защитить себя от атак социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) с помощью шифрования для защиты конфиденциальных данных;

2) путем проведения регулярных тренингов по повышению осведомленности сотрудников о безопасности;

3) полагаясь на антивирусное программное обеспечение для обнаружения атак;

4) путем внедрения строгого контроля доступа.

Задание 3. Выберите наиболее точное описание сути социальной инженерии.

Выберите все правильные ответы (один или несколько)

1) тип атаки, которая манипулирует людьми с целью разглашения конфиденциальной информации;

2) тип шифрования, который защищает личную информацию;

3) тип вируса, который заражает платформы социальных сетей;

4) тип программного обеспечения, которое используется для сбора персональных данных.

Задание 4. Что такое социальная инженерия и как она используется для компрометации информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) физическая атака на компьютерные сети;

2) тип программного обеспечения, используемого для кражи информации;

3) метод, используемый для манипулирования людьми с целью получения конфиденциальной информации;

4) тип шифрования, используемый для защиты информации.

Задание 5. Какие из перечисленных ниже методов социальной инженерии являются распространенными?

Выберите все правильные ответы (один или несколько)

1) мошенничество в социальных сетях;
2) фишинговые атаки;
3) заражение вредоносными программами;
4) все вышеперечисленное.

Задание 6. Что из приведенного ниже не является примером атаки социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) хакер получает доступ к системе, выдавая себя за представителя ИТ-службы поддержки;
2) хакер получает доступ к системе, выдавая себя за законного сотрудника;
3) хакер получает доступ к системе, взламывая слабый пароль;
4) хакер отправляет электронное письмо, которое, по-видимому, получено из законного источника, с запросом конфиденциальной информации.

Задание 7. Каковы некоторые распространенные методы, используемые в атаках социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) нарушения брандмауэра, DDoS-атаки и троянские кони;
2) взлом паролей, ботнеты и руткиты;
3) сканирование портов, мониторинг социальных сетей и прослушивание пакетов;
4) скрытый фишинг, травля и подлоги.

Задание 8. Каковы наилучшие методы предотвращения атак социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) информировать сотрудников об опасностях социальной инженерии;
2) используйте надежные пароли и двухфакторную аутентификацию;
3) поддерживать программное обеспечение и системы безопасности в актуальном состоянии;
4) все вышеперечисленное.

Задание 9. Что вам следует делать, если вы подозреваете, что стали жертвой атаки социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) сообщите об инциденте в ИТ-отдел вашей организации или в службу безопасности;

2) ничего, потому что нет никакого способа оправиться от атаки социальной инженерии;

3) немедленно измените все свои пароли;

4) удалите все электронные письма и файлы с вашего компьютера.

Задание 10. Каковы последствия того, что вы становитесь жертвой атаки социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) потеря персональных данных;

2) ущерб репутации;

3) финансовые потери;

4) все вышеперечисленное.

Задание 11. Почему социальная инженерия вызывает все большую озабоченность в современном обществе?

Выберите все правильные ответы (один или несколько)

1) из-за легкости доступа к личной информации в режиме онлайн;

2) из-за более широкого использования технологий и социальных сетей;

3) из-за растущей изощренности атак социальной инженерии;

4) из-за всего вышеперечисленного.

Задание 12. Каковы последствия для отдельных лиц и организаций, которые становятся жертвами атак социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) они могут столкнуться с судебными исками и финансовыми штрафами;

2) они могут потерять доступ к своим учетным записям и конфиденциальной информации;

3) они могут понести репутационный ущерб;

4) все вышеперечисленное.

Задание 13. Что могут сделать организации для предотвращения атак социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) проводить обучение сотрудников по вопросам безопасности;
2) внедрить строгий контроль доступа и меры аутентификации;
3) проводить регулярные оценки и аудиты безопасности;
4) все вышеперечисленное.

Задание 14. Что из приведенного ниже является примером предлога?

Выберите все правильные ответы (один или несколько)

1) отправка электронного письма с поддельной страницей входа для кражи пароля пользователя;
2) выдавать себя за представителя службы поддержки клиентов для получения конфиденциальной информации;
3) использование атаки методом перебора для угадывания пароля пользователя;
4) использование USB-накопителя для заражения компьютера вредоносным ПО.

Задание 15. Что из приведенного ниже является примером атаки социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) взлом сети с использованием атаки методом перебора;
2) установка вируса на компьютер;
3) проникновение в здание с целью кражи компьютера;
4) использование фишингового электронного письма, чтобы обманом заставить кого-либо ввести свой пароль.

Задание 16. Какова распространенная тактика, используемая в атаках социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) нарушения брандмауэра;
2) SQL-инъекции;
3) атаки с применением грубой силы;
4) фишинговые электронные письма.

Задание 17. Что могут сделать отдельные люди, чтобы защитить себя от атак социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) поддерживать программное обеспечение и системы безопасности в актуальном состоянии;

2) использовать надежные пароли и двухфакторную аутентификацию;

3) быть осторожными с нежелательными электронными письмами или сообщениями;

4) все вышеперечисленное.

Задание 18. Как можно предотвратить атаки социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) путем установки антивирусного программного обеспечения;

2) путем информирования сотрудников о рисках и о том, как распознавать атаки социальной инженерии;

3) путем шифрования всех данных в сети;

4) используя надежные пароли.

Задание 19. Каковы юридические и этические последствия атак социальной инженерии?

Выберите все правильные ответы (один или несколько)

1) они незаконны и неэтичны;

2) они являются законными и этичными;

3) они законны, но неэтичны;

4) они незаконны, но этичны.

Задание 20. Каково влияние атак социальной инженерии на общество?

Выберите все правильные ответы (один или несколько)

1) они могут привести к перебоям в подаче электроэнергии и другим сбоям в работе инфраструктуры;

2) они могут привести к потере персональных данных;

3) они могут привести к финансовым потерям и краже личных данных;

4) они могут привести к физическому повреждению компьютерных систем.

ГЛАВА 41. ЦИФРОВИЗАЦИЯ ОБЩЕСТВА: ПРЕДПОСЫЛКИ, ТЕНДЕНЦИИ, ПЕРСПЕКТИВЫ

Задание 1. Какова роль правительства в продвижении и регулировании цифровизации?

Выберите все правильные ответы (один или несколько)

1) регулировать использование цифровых технологий для обеспечения справедливости и равноправия;

2) препятствовать внедрению цифровых технологий для защиты традиционных отраслей промышленности;

3) содействовать внедрению цифровых технологий для ускорения экономического роста;

4) ограничить доступ к цифровым технологиям для защиты конфиденциальности и безопасности.

Задание 2. Каковы этические соображения, связанные с цифровизацией?

Выберите все правильные ответы (один или несколько)

1) честность и равноправие;

2) конфиденциальность и защита данных;

3) прозрачность и подотчетность;

4) все вышеперечисленное.

Задание 3. Что такое цифровизация?

Выберите все правильные ответы (один или несколько)

1) процесс создания физических копий цифровой информации;

2) процесс подключения электронных устройств к сети;

3) процесс преобразования цифровых данных в аналоговую информацию;

4) процесс преобразования аналоговой информации в цифровые данные.

Задание 4. Какой термин описывает неравномерное распределение цифровых ресурсов в обществе?

Выберите все правильные ответы (один или несколько)

1) цифровой разрыв;

2) цифровой доступ;

3) расширение прав и возможностей в области цифровых технологий;

4) цифровое исключение.

Задание 5. Каковы потенциальные риски цифровизации для общества?

Выберите все правильные ответы (один или несколько)

1) расширение доступа к информации и услугам;
2) снижение уровня конфиденциальности и защиты данных;
3) расширение возможностей для инноваций и творчества;
4) усиление социального и экономического неравенства.

Задание 6. Каковы потенциальные преимущества цифровизации для общества?

Выберите все правильные ответы (один или несколько)

1) ограниченные возможности для инноваций и творчества;
2) повышенная конфиденциальность и защита данных;
3) сокращение социального и экономического неравенства;
4) улучшение доступа к информации и услугам.

Задание 7. Какое потенциальное влияние цифровизации на будущее образования?

Выберите все правильные ответы (один или несколько)

1) снижение значимости образования и профессиональной подготовки;
2) ограниченное воздействие на образование и профессиональную подготовку;
3) повышенное внимание к традиционным формам образования и профессиональной подготовки;
4) расширение доступа к образованию и профессиональной подготовке.

Задание 8. Каковы основные факторы, способствующие цифровому неравенству?

Выберите все правильные ответы (один или несколько)

1) знакомство с иностранными языками;
2) возраст, пол и уровень дохода;
3) политическая принадлежность и социальный статус;
4) доступ к тренажерным залам.

Задание 9. Укажите новые технологии и тенденции в области цифровизации.

Выберите все правильные ответы (один или несколько)

1) искусственный интеллект и машинное обучение;
2) блокчейн и криптовалюта;
3) виртуальная и дополненная реальность;
4) все вышеперечисленное.

Задание 10. Какая группа с наибольшей вероятностью столкнется с цифровым неравенством?

Выберите все правильные ответы (один или несколько)

1) пожилые люди;
2) студенты колледжа;
3) профессионалы в высокотехнологичных отраслях промышленности;
4) маленькие дети.

Задание 11. Как цифровое неравенство влияет на отдельных людей и сообщества?

Выберите все правильные ответы (один или несколько)

1) цифровое неравенство поощряет социальные взаимодействия и создание сетей;
2) цифровое неравенство может ограничить возможности получения образования и трудоустройства;
3) цифровое неравенство способствует конфиденциальности и безопасности в Интернете;
4) цифровое неравенство расширяет доступ к достоверной информации.

Задание 12. Что из перечисленного является примером цифрового неравенства?

Выберите все правильные ответы (один или несколько)

1) подросток, проводящий слишком много времени в социальных сетях;
2) физическое лицо, загружающее мобильное приложение для личного использования;
3) студент, использующий онлайн-ресурсы для проведения исследований;
4) человек, у которого дома нет доступа в Интернет.

Задание 13. Что такое цифровое неравенство?

Выберите все правильные ответы (один или несколько)

1) наличие высокоскоростного интернета в сельской местности;
2) использование платформ социальных сетей для онлайн-общения;
3) разрыв между доступом людей к цифровым технологиям и ресурсам;
4) уровень цифровых навыков и грамотности в данной популяции.

Задание 14. Какую роль играет образование в сокращении цифрового неравенства?

Выберите все правильные ответы (один или несколько)

1) образование фокусируется только на автономных навыках и знаниях;
2) образование усугубляет цифровое неравенство;
3) образование никак не влияет на цифровое неравенство;
4) образование может помочь преодолеть цифровой разрыв.

Задание 15. Отметьте потенциальные проблемы полностью цифрового общества.

Выберите все правильные ответы (один или несколько)

1) зависимость от цифровых технологий;
2) усиление социального и экономического неравенства;
3) ограниченные возможности для инноваций и творчества;
4) все вышеперечисленное.

Задание 16. Какое влияние может потенциально оказать цифровизация на традиционные отрасли и бизнес-модели?

Выберите все правильные ответы (один или несколько)

1) повышение гарантий занятости и стабильности в традиционных отраслях промышленности;
2) разрушение и трансформация традиционных отраслей промышленности;
3) ограниченное воздействие на традиционные отрасли промышленности;
4) ликвидация всех традиционных отраслей промышленности.

Задание 17. Отметьте стратегии борьбы с цифровым неравенством.

Выберите все правильные ответы (один или несколько)

1) поощрение оффлайн-активности и сведение к минимуму присутствия в Интернете;
2) предоставление свободного доступа к цифровым устройствам и ресурсам;
3) ограничение доступности онлайн-контента;
4) увеличение стоимости интернет-услуг.

Задание 18. Какой термин относится к разрыву в цифровых навыках и знаниях между различными людьми и группами?

Выберите все правильные ответы (один или несколько)

1) цифровая грамотность;
2) цифровое исключение;
3) цифровая компетентность;
4) цифровой разрыв.

Задание 19. Какая роль образования и грамотности в содействии успешной цифровизации?

Выберите все правильные ответы (один или несколько)

1) ограничить доступ к цифровым технологиям для защиты конфиденциальности и безопасности;

2) содействовать внедрению цифровых технологий для ускорения экономического роста;

3) препятствовать внедрению цифровых технологий для защиты традиционных отраслей промышленности;

4) создать квалифицированную рабочую силу, способную использовать цифровые технологии.

ГЛАВА 42. НОРМАТИВНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ И ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА

Задание 1. Как новые технологии влияют на правила информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) они делают ненужными правила информационной безопасности;
2) они создают новые риски и вызовы в области кибербезопасности;
3) они не оказывают влияния на правила информационной безопасности;
4) они уменьшают потребность в правилах информационной безопасности.

Задание 2. Какая из перечисленных ниже методик является общепринятой для проведения оценки рисков в области управления рисками информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) SWOT-анализ;
2) анализ первопричин (RCA);
3) анализ режимов отказов и последствий (FMEA);
4) методика Delphi.

Задание 3. Какова основная цель учета рисков при управлении рисками информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) передавать риски третьей стороне;
2) снизить риски до приемлемого уровня;
3) устранить все риски;
4) игнорировать риски, которые считаются незначительными.

Задание 4. Что из перечисленного является потенциальным преимуществом использования искусственного интеллекта в управлении рисками информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) повышенное внимание к принятию рисков, а не к их смягчению;
2) повышение точности и скорости оценки рисков;
3) более активное вмешательство человека в процессы управления рисками;
4) сокращение потребности в мониторинге и пересмотре рисков.

Задание 5. Какова роль правовых норм в обеспечении информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) информирование общественность о киберугрозах;
2) наказание киберпреступников;
3) предотвращение всех кибератак;
4) создание основы для защиты информационных активов.

Задание 6. Какой международный стандарт безопасности создан специально для защиты данных платежных карт?

Выберите все правильные ответы (один или несколько)

1) PCI DSS;
2) COBIT;
3) HIPAA;
4) ISO 9001.

Задание 7. Как законы о неприкосновенности частной жизни влияют на информационную безопасность?

Выберите все правильные ответы (один или несколько)

1) они ограничивают сбор, использование и хранение личной информации;
2) они повышают риск кибератак;
3) они не оказывают влияния на информационную безопасность;
4) они поощряют компании делиться личной информацией с третьими лицами.

Задание 8. Какова основная цель создания эффективной программы управления рисками информационной безопасности в организации?

Выберите все правильные ответы (один или несколько)

1) устранить все риски;
2) передать все риски третьей стороне;
3) игнорировать риски, которые считаются незначительными;
4) снизить риски до приемлемого уровня.

Задание 9. В чем заключается основное преимущество наличия международных соглашений и сотрудничества в области информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) в создании новых технологий кибербезопасности;
2) в способствовании кибератакам;
3) в обеспечении согласованного регулирования на всех границах;
4) в ограничении конкуренции между странами.

Задание 10. Какая из перечисленных ниже проблем является распространенной в управлении рисками информационной безопасности, связанными с человеческим фактором?

Выберите все правильные ответы (один или несколько)

1) технические уязвимости;
2) физическая безопасность;
3) недостаточная подготовка и осведомленность;
4) недостаточный бюджет и ресурсы.

Задание 11. Что из перечисленного является потенциальной угрозой при управлении рисками информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) антивирусное программное обеспечение;
2) технология шифрования;
3) внедрение брандмауэра;
4) атаки социальной инженерии.

Задание 12. Какова основная цель нормативно-правовых норм в обеспечении информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) защита персональных данных;
2) поощрение утечек данных;
3) ограничение свободы выражения мнений;
4) поощрение киберпреступности.

Задание 13. Какова главная цель международного сотрудничества в области информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) содействовать расширению сотрудничества между странами в области защиты от киберугроз;
2) создать единый свод законов и нормативных актов в области кибербезопасности;
3) увеличить количество кибератак по всему миру;
4) создать глобальные силы кибербезопасности.

Задание 14. Как законы о конфиденциальности влияют на информационную безопасность?

Выберите все правильные ответы (один или несколько)

1) они способствуют обмену личными данными между организациями;
2) они поощряют сбор и использование персональных данных без ограничений;
3) они ограничивают сбор, использование и хранение персональных данных;
4) они не оказывают влияния на информационную безопасность.

Задание 15. Что из приведенного ниже является примером технического контроля в управлении рисками информационной безопасности?

Выберите все правильные ответы (один или несколько)

1) внедрение брандмауэра;
2) планирование реагирования на инциденты;
3) проверка биографических данных;
4) обучение по вопросам безопасности.

ГЛАВА 43. МЕЖДУНАРОДНАЯ БЕЗОПАСНОСТЬ КАК СФЕРА МИРОВОГО ВЗАИМОДЕЙСТВИЯ

Задание 1. К важным причинам обострения российско-американского противостояния относятся:

Выберите все правильные ответы (один или несколько)

1) расширение НАТО;
2) расширение военного сотрудничества США и Японии;
3) ядерная и космическая политика США;
4) развязанные США и НАТО войны в Сирии, Ираке и Афганистане;
5) развертывание США системы стратегической противоракетной обороны.

Задание 2. _____ – это защищенность мирового сообщества или группы государств от возможности нанесения им ущерба средствами вооруженного насилия, обеспечиваемая их совместными усилиями. (вписать пропущенные два слова)

Задание 3. Понятие «коллективная безопасность» получило распространение:

Выберите все правильные ответы (один или несколько)

1) в 1950-е гг.;
2) в 1970-е гг.;
3) в 1920-е гг.;
4) в 1890-е гг.

Задание 4. Комплекс взаимосвязанных межгосударственных отношений и организаций, политико-дипломатических, экономических, военных и общественных мероприятий и усилий, обеспечивающих коллективную безопасность государств и народов – это:

Выберите все правильные ответы (один или несколько)

1) региональная безопасность;
2) глобальное управление;
3) национальные интересы;
4) система международной безопасности.

Задание 5. _____ – это состояние международных отношений, исключающее нарушение всеобщего мира или создание угрозы безопасности народов, государств, межгосударственных объединений в какой бы то ни было форме. (вписать пропущенные два слова)

Задание 6. Особенности гибридной войны:

Выберите все правильные ответы (один или несколько)

1) сложность прогнозирования последствий конфликта;
2) свойство увеличения масштабов;
3) нелигитимность;
4) неопределенность сторон конфликта;
5) высокая степень географической локализации;
6) значительная сложность завершения.

Задание 7. Противостояние США и СССР во второй половине XX в. рассматривалось:

Выберите все правильные ответы (один или несколько)

1) как «игра с нулевой суммой»;
2) как кооперативная игра;
3) как «игра с проигрышем»;
4) как «игра с зеркалом».

Задание 8. Основной целью государства защиту естественных прав людей на жизнь, свободу и собственность считал:

Выберите все правильные ответы (один или несколько)

1) Т. Гоббс;
2) Дж. Локк;
3) Н. Макиавелли;
4) Г. Гроций.

Задание 9. Для детерминантов в сфере обеспечения международной безопасности второй категории характерны:

Выберите все правильные ответы (один или несколько)

1) долговременный характер длительности действия;
2) кратковременный характер длительности действия;
3) страна как географическое измерение;
4) глобальное географическое измерение;
5) среднесрочный характер длительности действия;
6) регион как географическое измерение.

Задание 10. Автором термина «столкновение цивилизаций» является:
Выберите все правильные ответы (один или несколько)

1) Р. Робертсон;
2) С. Хантингтон;
3) Р. Куглер;
4) У. Бек.

Задание 11. _____ – это официальные институты и организации, которыми создаются и поддерживаются правила и нормы, управляющие мировым порядком, а также все те организации и группы влияния, которые преследуют цели, достижение которых зависит от транснациональных центров влияния. (вписать пропущенные два слова)

Задание 12. Какие угрозы международной безопасности выделяет СНГ?
Выберите все правильные ответы (один или несколько)

1) преступления в сфере информационных технологий;
2) организованная международная преступность, в том числе незаконный оборот оружия, наркотических средств и психотропных веществ;
3) проблема «несостоявшихся государств»;
4) этнические и религиозные конфликты;
5) международный терроризм и экстремизм.

Задание 13. _____ в сфере обеспечения национальной безопасности представляет собой возможность наступления негативных последствий в результате принятия и реализации социальными факторами и институтами политических решений на национальном и межгосударственном уровне. (вписать пропущенные два слова)

Задание 14. «Сжатием» мира и усилением взаимозависимости всех его частей, что сопровождается все более распространенным осознанием целостности, единства мира, называет Р. Робертсон:
Выберите все правильные ответы (один или несколько)

1) интеграцию;
2) регионализацию;
3) глобализацию;
4) секторализацию.

Задание 15. _____ это способ военных действий, в основе которого лежит расчет на достижение победы путем последовательного ослабления противника, истощения его вооруженных сил, лишения противника возможности восстановить потери и удовлетворять военные нужды, поддерживать боеспособность армии на требуемом уровне, перехватывать его коммуникации, принуждать врага к капитуляции. (вписать пропущенные два слова)

ГЛАВА 44. ТЕСТ ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ В МНОГОПОЛЯРНОМ МИРЕ

Задание 1. Внешние проявления процессов деятельности международной организации по выполнению возложенных на нее задач – это:

Выберите все правильные ответы (один или несколько)

1) принципы;
2) методы;
3) цели;
4) функции.

Задание 2. Постоянными членами Совета Безопасности ООН являются:

Выберите все правильные ответы (один или несколько)

1) Россия;
2) Китай;
3) Япония;
4) Индия;
5) Бразилия;
6) Германия;
7) Великобритания;
8) Франция;
9) США.

Задание 3. В Совет Безопасности ООН входят:

Выберите все правильные ответы (один или несколько)

1) 15 государств;
2) 11 государств;
3) 9 государств;
4) 5 государств.

Задание 4. Реформирование ООН должно отвечать следующим объективным тенденциям:

Выберите все правильные ответы (один или несколько)

1) совершенствование нормативно-правовой базы;
2) построение более широкой концепции коллективной безопасности;
3) укрепления традиционных инструментов реагирования ООН;
4) всеобъемлющий характер трансформации;
5) сокращение числа постоянных членов Совета Безопасности и ликвидация института права вето.

Задание 5. Сколько миротворческих операций учредила ООН в период с 1945 по 1985 г.?

Выберите все правильные ответы (один или несколько)

1) 13;
2) 5;
3) 34;
4) ни одной.

Задание 6. Устав ООН был принят в Сан-Франциско:

Выберите все правильные ответы (один или несколько)

1) 10 декабря 1948 г.;
2) 26 июня 1945 г.;
3) 24 октября 1949 г.;
4) 16 декабря 1954 г.

Задание 7. Согласно Уставу ООН, главная ответственность за поддержание международного мира и безопасности возложена:

Выберите все правильные ответы (один или несколько)

1) на Генерального секретаря ООН;
2) на Генеральную Ассамблею ООН;
3) на Совет Безопасности ООН;
4) на Международный суд ООН.

Задание 8. Не связанные с использованием вооруженных сил меры, которые могут применяться для осуществления решении Совета Безопасности ООН, включают:

Выберите все правильные ответы (один или несколько)

1) разрыв дипломатических отношений;
2) полный или частичный перерыв железнодорожных, морских, воздушных, почтовых, телеграфных, радио или других средств сообщения;
3) ВЫВОД ВОЙСК;
4) полный или частичный перерыв экономических отношений;
5) блокаду.

Задание 9. В состав Лиги арабских государств входят:

Выберите все правильные ответы (один или несколько)

1) 17 участников;
2) 22 участника;
3) 14 участников;
4) 9 участников.

Задание 10. Общее политическое руководство ЕС осуществляет:

Выберите все правильные ответы (один или несколько)

1) Европейский Совет;
2) Европейский парламент;
3) Совет;
4) Европейская Комиссия;
5) Генеральный секретарь.

Задание 11. Характерные черты региональных систем коллективной безопасности:

Выберите все правильные ответы (один или несколько)

1) предусматривается обязанность участников оказывать индивидуальную или коллективную помощь государству, подвергшемуся вооруженному нападению извне;

2)о принятых мерах коллективной обороны немедленно извещается СБ ООН;

3) принятие новых государств в установленную договором систему безопасности возможно только по приглашению одного из ее участников;

4) закрепляется обязательство участников договора решать споры между собой исключительно мирными средствами.

Задание 12. Действующими региональными организациями, участвующими в поддержании безопасности, являются:

Выберите все правильные ответы (один или несколько)

1) ОВД;
2) НАТО;
3) ОБСЕ;
4) ОДКБ;
5) ШОС.

Задание 13. Главными институтами Европейского Союза являются:

Выберите все правильные ответы (один или несколько)

1) Секретариат;
2) Европейская Комиссия;
3) Совет;
4) Европейский Совет;
5) Европейский парламент;
6) Суд ЕС;
7) Европейский центральный банк.

Задание 14. Членами Организации Договора о коллективной безопасности являются:

Выберите все правильные ответы (один или несколько)

1) Узбекистан;
2) Грузия;
3) Белоруссия;
4) Киргизия;
5) Таджикистан;
6) Казахстан;
7) Россия;
8) Армения;
9) Азербайджан.

Задание 15. Содружество Независимых Государств было основано:

Выберите все правильные ответы (один или несколько)

1) в 1991 г.;
2) в 1992 г.;
3) в 1990 г.;
4) в 1993 г.

Задание 16. Органами ОДКБ являются:

Выберите все правильные ответы (один или несколько)

1) Совет министров обороны;
2) Совет коллективной безопасности;
3) Совет министров иностранных дел;
4) Комитет секретарей советов безопасности;
5) Совет глав государств.

Задание 17. Договор о создании Союзного государства между Российской Федерацией и Республикой Беларусь был подписан:

Выберите все правильные ответы (один или несколько)

1) в 2012 г.;
2) в 1999 г.;
3) в 1995 г.;
4) в 2005 г.

Задание 18. Основным исполнительным органом СНГ является:

Выберите все правильные ответы (один или несколько)

1) Совет глав государств;
2) Совет глав правительств;
3) Экономический совет;
4) Совет министров иностранных дел.

Задание 19. Высшим руководящим органом Африканского Союза является:

Выберите все правильные ответы (один или несколько)

1) Панафрийский парламент;
2) Исполнительный совет министров;
3) Ассамблея глав государств и правительств;
4) Постоянный комитет представителей.

Задание 20. Постоянная структурированная сотрудничество по вопросам безопасности и обороны было учреждено:

Выберите все правильные ответы (один или несколько)

1) ОАГ;
2) ЕС;
3) ОБСЕ;
4) НАТО.

Задание 21. Особенности ОБСЕ, как организации, призваны обеспечивать международную безопасность:

Выберите все правильные ответы (один или несколько)

1) отсутствие у стран членов права вета;
2) отсутствие полномочий санкционировать действия других региональных организаций по «принуждению к миру»;
3) отсутствие права принимать решение о применении мер принудительного характера;
4) отсутствие собственных вооруженных сил.

ГЛАВА 45. НАТО

Задание 1. К странам-основателям НАТО относятся:
Выберите все правильные ответы (один или несколько)

1) Великобритания;
2) Дания;
3) Бельгия;
4) Исландия;
5) Польша;
6) Люксембург;
7) ФРГ.

Задание 2. В основе отношений членов НАТО лежит принцип, согласно которому:
Выберите все правильные ответы (один или несколько)

1) в любой операции принимают участие все члены Альянса;
2) нападение на любого члена требует незамедлительного противодействия;
3) нападение на одного или на нескольких из его членов рассматривается как нападение на них всех;
4) обеспечивается глобальный масштаб безопасности.

Задание 3. Организация Североатлантического договора была основана:
Выберите один правильный ответ

1) в 1954 г.;
2) в 1952 г.;
3) в 1966 г.;
4) в 1949

Задание 4. Штаб-квартира НАТО находится:
Выберите все правильные ответы (один или несколько)

1) в Нью-Йорке;
2) в Лондоне;
3) в Вашингтоне;
4) в Брюсселе.

Задание 5. Генеральный секретарь НАТО назначается:
Выберите все правильные ответы (один или несколько)

1) на 6 лет;
2) на 2 года;
3) на 8 лет;
4) на 4 года.

Задание 6. Главными политическими и руководящими органами НАТО являются:

Выберите все правильные ответы (один или несколько)

1) Комитет военного планирования;
2) Парламентская ассамблея;
3) Группа ядерного планирования;
4) Комитет по операциям;
5) Североатлантический совет.

Задание 7. Сессии Североатлантического совета на уровне министров обычно проводятся:

Выберите все правильные ответы (один или несколько)

1) ежемесячно;
2) ежеквартально;
3) не реже двух раз в год;
4) не реже трех раз в полугодие.

Задание 8. Сколько постоянных объединенных штабов оперативного звена существует в НАТО?

Выберите все правильные ответы (один или несколько)

1) три;
2) девять;
3) пять;
4) семь.

Задание 9. Задачи поддержания и развития связей НАТО с восточно-европейскими государствами возложены:

Выберите все правильные ответы (один или несколько)

1) на Североатлантический совет;
2) на Ассоциацию Атлантического договора;
3) на Совет евроатлантического партнерства;
4) на Парламентскую ассамблею НАТО.

Задание 10. Ключевые мероприятия по внутренней адаптации НАТО:

Выберите все правильные ответы (один или несколько)

1) повышение экспедиционного потенциала ОВС НАТО;
2) снижение нормативов по срокам развертывания резервного компонента;
3) реформирование командной структуры ОВС НАТО;
4) наращивание потенциала воздушно-космических средств нападения и обороны.

Задание 11. Франция не участвовала в военной организации НАТО в период:

Выберите все правильные ответы (один или несколько)

1) с 1966 по 2009 гг.;
2) с 1982 по 2012 гг.;
3) с 1952 по 1999 гг.;
4) с 1999 по 2017 гг.

Задание 12. В каком городе ЕС и НАТО совместно открыли в 2017 г. Европейский центр передового опыта по противодействию гибридным угрозам?

Выберите все правильные ответы (один или несколько)

1) в Хельсинки;
2) в Праге;
3) в Риге;
4) в Стокгольме.

Задание 13. Участниками Средиземноморского диалога являются:

Выберите все правильные ответы (один или несколько)

1) Иордания;
2) Тунис;
3) Крит;
4) Израиль;
5) Марокко;
6) Египет;
7) Сирия.

Задание 14. Согласно достигнутым договоренностям, члены НАТО обязались тратить на военные расходы не менее:

Выберите все правильные ответы (один или несколько)

1) 2 % ВВП;
2) 5 % ВВП;
3) 1 % ВВП;
4) 0,5 % ВВП.

Задание 15. Протокол о присоединении страны к НАТО должен быть утвержден:

Выберите все правильные ответы (один или несколько)

1) странами-основателями НАТО;
2) всеми государствами – членами НАТО;
3) простым большинством государств – членов НАТО;
4) квалифицированным большинством государств – членов НАТО.

Задание 16. Проект акта «О консолидации свободы в НАТО», открывшего возможности по вступлению в НАТО для Грузии, Украине, Албании, Македонии и Хорватии, был утвержден:

Выберите все правильные ответы (один или несколько)

1) в 2007 г.;
2) в 2018 г.;
3) в 1999 г.;
4) в 2011 г.

Задание 17. Основные причины развития инициатив НАТО в регионах Ближнего Востока и Северной Африки:

Выберите все правильные ответы (один или несколько)

1) увеличение объемов торговли наркотиками в Средиземноморском регионе;

2) возросшая политическая, экономическая и военная активность России и других государств в странах Средиземноморья;

3) неконтролируемая миграция через Средиземное море;

4) распространение ОМУ и средств его доставки, международного терроризма, рост организованной преступности в Средиземноморском регионе.

ГЛАВА 46. МОДЕЛИ И МЕХАНИЗМЫ МИРОВОГО ПОЛИТИЧЕСКОГО РАЗВИТИЯ

Задание 1. В зависимости от масштаба и количества субъектов, формирующих систему обеспечения международной безопасности, выделяют следующие модели:

Выберите все правильные ответы (один или несколько)

1) глобальные;
2) кооперативные;
3) субрегиональные;
4) региональные;
5) локальные.

Задание 2. Сопоставьте содержание системных элементов модели обеспечения международной безопасности.

Процессор	Обеспечение сопоставления текущего состояния международной безопасности с ее заданным уровнем
Выход	Реализация задач обмена информацией, контроля, управления и обратной связи между различными уровнями управления модели
Функция	Раскрывает предназначение модели и отражает процессы выработки решений, направленных на снижение уровня конфликтности в межгосударственных отношениях, обеспечение военно-стратегической устойчивости в мире и создание условий для расширения сотрудничества между различными государствами и нациями
ВХОД	Различные факторы, связанные с выбранной стратегией обеспечения международной безопасности, желаемым сценарием развития обстановки и политическими ситуациями, возникающими в рамках сценария

Задание 3. Классификацию видов политической адаптации, которая на основе системного подхода позволяет установить связи между внешней политикой государства и системой международных отношений, предложил:

Выберите все правильные ответы (один или несколько)

1) М. Мерль;
2) Г. Моргентау;
3) О Р. Кеохейн;
4) Д. Розенау.

Задание 4. Классифицируйте идеальные модели по различным основаниям. Соедините элементы попарно цифры с буквами.

Выберите все правильные ответы (один или несколько)

1) уровень моделируемой системы;
2) уровень формализации;
3) ориентированность на воспроизведение оригинала;
4) место в структуре научного познания.

а) микро- и макромодели;
б) концептуальные и формально-логические модели;
в) описательные, объяснительные, предсказательные и критериальные модели;
г) субстанциональные, структурные, функциональные модели.

Задание 5. Основные типы политических адаптивных стратегий:

Выберите все правильные ответы (один или несколько)

1) предохранительная адаптация;
2) уступчивая адаптация;
3) неуступчивая адаптация;
4) интегративная адаптация.

Задание 6. К современным «центрам силы» относят:

Выберите все правильные ответы (один или несколько)

1) Канаду;
2) Россию;
3) Китай;
4) США;
5) ЕС;
6) Бразилию.

Задание 7. _____ обеспечения международной безопасности – это идеальный образ, аналог международной политической/военно-политической организации или совокупности взаимодействующих организаций, воспроизводящий в символической форме присущие организации типические черты. (вписать пропущенное слово).

Задание 8. Автором неолиберального сценария развития процессов глобализации является:

Выберите все правильные ответы (один или несколько)

1) С. Хоффман;
2) С. Хантингтон;
3) Ф. Брайар;
4) Ф. Фукуяма.

Задание 9. Характерные особенности концептуального моделирования, которые позволяют использовать его для решения задач построения модели:

Выберите все правильные ответы (один или несколько)

1) связи между переменными задаются с помощью выражений на естественном языке;

2) критерии выбора описываются качественными рекомендациями по предпочтительности, недопустимости или желательности того или иного варианта решения;

3) связи между переменными выражаются в виде математических уравнений;

4) переменные в концептуальных моделях не количественные, а качественные.

Задание 10. Стратегия национальной безопасности РФ относит к стратегическим национальным приоритетам:

Выберите все правильные ответы (один или несколько)

1) повышение качества жизни российских граждан;
2) оборону страны;
3) здравоохранение;
4) государственную и общественную безопасность;
5) демократическое развитие всех властных институтов;
6) равноправное стратегическое партнерство.

Задание 11. _____ – это добровольное ограничение личностью, государством или коалицией собственных потребностей, интересов. (вписать пропущенное слово)

Задание 12. По мнению академика РАН В. Барановского, актуальным является формирование нового миропорядка, основанного:

Выберите все правильные ответы (один или несколько)

1) на балансе потребностей;
2) на балансе интересов;
3) на балансе возможностей;
4) на балансе сил.

Задание 13. Элементами адаптивной интегративной модели международной безопасности России выступают:

Выберите все правильные ответы (один или несколько)

1) контур мониторинга;
2) канал текущего взаимодействия;
3) контур обеспечения национальной безопасности России;
4) контур противодействия;
5) контур организаций обеспечения международной безопасности;
6) канал обратной связи.

Задание 14. Устойчивость интегративной модели международной безопасности России за счет адаптации и балансировки результатов деятельности по обеспечению международной безопасности, которые отражаются на выходе модели. обеспечивает:

Выберите все правильные ответы (один или несколько)

1) блок конструктивных организаций;
2) блок национальных ценностей;
3) блок СНП;
4) канал обратной связи.

ГЛАВА 47. АВТОРСКОЕ ПРАВО. ОХРАНА АВТОРСКОГО ПРАВА ГОСУДАРСТВОМ

Задание 1. Оригинал картины был продан художником частному лицу. Имеет ли художник право публиковать репродукции этой картины?

Выберите все правильные ответы (один или несколько)

1) нет, не имеет. Права на воспроизведение переходят к новому правообладателю;

2) имеет, но только в случае согласия нового владельца картины;

3) да, имеет.

Задание 2. Авторами аудиовизуального произведения являются:

Выберите все правильные ответы (один или несколько)

1) актеры;

2) композитор;

3) автор сценария;

4) режиссер-постановщик;

5) исполнители музыки.

Задание 3. Авторские права на программы для ЭВМ подлежат защите:

Выберите все правильные ответы (один или несколько)

1) как права на объекты промышленной собственности;

2) так же, как и права на литературные произведения;

3) либо как права на литературные произведения, либо как права на промышленный образец, в зависимости от обстоятельств создания программы.

Задание 4. К авторскому праву относятся права на:

Выберите все правильные ответы (один или несколько)

1) фотографию;

2) симфонию;

3) повесть;

4) логотип;

5) дизайн.

Задание 5. Авторское право на музыкальное произведение возникает:

Выберите все правильные ответы (один или несколько)

1) после регистрации прав на него в ВААП;

2) при его создании;

3) после его публикации (исполнения).

Задание 6. Право _____ состоит в том, что автор произведения изобразительного искусства имеет право на получение вознаграждения в виде процентных отчислений от цены перепродажи оригинала произведения. (вписать пропущенное слово)

Задание 7. Исключительное право на произведение действует:

Выберите все правильные ответы (один или несколько)

1) в течение всей жизни автора и 100 лет после его смерти;
2) в течение всей жизни автора и 40 лет после его смерти;
3) в течение всей жизни автора и 70 лет после его смерти;
4) в течение всей жизни автора и 50 лет после его смерти.

Задание 8. Снятие информации с технических каналов связи не разрешено:

Выберите все правильные ответы (один или несколько)

1) ФСБ;
2) частным охранным предприятиям при наличии лицензии;
3) таможенным органам;
4) органам внутренних дел РФ;
5) ФСО.

Задание 9. Без согласия автора репродукция картины может быть опубликована:

Выберите все правильные ответы (один или несколько)

1) если такая публикация не была специально запрещена автором или иным правообладателем;
2) в периодической печати в информационных целях;
3) в учебной литературе в качестве иллюстрации.

ГЛАВА 48. РОЛИ И ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ ПО РАЗРАБОТКЕ И ВНЕДРЕНИЮ ПОЛИТИКИ БЕЗОПАСНОСТИ

Задание 1. Совокупность наиболее значимых решений, направленных на обеспечение приемлемого уровня безопасности функционирования предприятия, – это:

Выберите все правильные ответы (один или несколько)

1) система безопасности;
2) политика безопасности;
3) стратегия безопасности.

Задание 2. Для обеспечения защиты информации, содержащейся в информационной системе, применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии с Федеральным законом:

Выберите все правильные ответы (один или несколько)

1) Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах;
2) Об информации, информационных технологиях и о защите информации;
3) О техническом регулировании.

Задание 3. Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации информационной системы, должны быть направлены на обеспечение конфиденциальности, _____ и доступности информации. (вписать пропущенное слово)

Задание 4. Разработку и внедрение систем защиты информации условно можно разделить на 4 основных этапа:

Выберите все правильные ответы (один или несколько)

1) требования и критерии систем защиты информации;
2) разработка;
3) внедрение;
4) аттестация.

Задание 5. Типовая политика безопасности предполагает:

Выберите все правильные ответы (один или несколько)

1) открытое взаимодействие с Интернетом, отдельную обработку наиболее важных данных;

2) разделение внешних и внутренних систем с помощью брандмауэра, сохранение доступности интернет-служб для внутренних пользователей;

3) вынос взаимодействия с Интернетом в отдельную систему, не связанную с внутренней сетью организации.

Задание 6. Описание того, где, как, когда, кем и для чего используется политика безопасности, характеризует:

Выберите все правильные ответы (один или несколько)

1) предмет политики;
2) применимость политики;
3) позицию организации;
4) соблюдение политики.

ГЛАВА 49. КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ

Задание 1. Из технических каналов перехвата информации по кабельным каналам связи наиболее часто используются:

Выберите все правильные ответы (один или несколько)

1) электромагнитные;
2) индукционные;
3) электрические.

Задание 2. Дальность действия «лазерных микрофонов» составляет:

Выберите все правильные ответы (один или несколько)

1) несколько сотен метров;
2) до сотни метров;
3) несколько десятков метров.

Задание 3. «Микрофонный эффект» может возникать при использовании таких вспомогательных технических средств как:

Выберите все правильные ответы (один или несколько)

1) электробытовые приборы;
2) громкоговорители ретрансляционной сети;
3) датчики пожарной сигнализации;
4) системы отопления и водоснабжения.

Задание 4. Технический канал утечки информации путем «высокочастотного навязывания» наиболее часто используют для перехвата разговоров, ведущихся в помещении:

Выберите все правильные ответы (один или несколько)

1) через сети электропитания;
2) через телефонный аппарат;
3) через системы отопления и водоснабжения.

Задание 5. Параметрический канал утечки информации формируется путем:

Выберите все правильные ответы (один или несколько)

1) съема информации с использованием закладных устройств;
2) улавливания наводки электромагнитных излучений ТСОИ;
3) высокочастотного облучения ТСОИ;
4) съема информационных сигналов, просачивающихся в цепи электропитания.

Задание 6. Электромагнитные излучения элементов ТСОИ, носителем информации является электрический ток, сила которого, напряжение, частота или фаза изменяются по закону информационного сигнала, могут использоваться для съема информации:

Выберите все правильные ответы (один или несколько)

1) с сетевых подключений;
2) с дисплея по электромагнитному каналу;
3) с принтера по каналу связи с компьютером;
4) за счет побочного излучения терминала.

ГЛАВА 50. ТЕХНИЧЕСКИЕ СРЕДСТВА БОРЬБЫ С ПРОМЫШЛЕННЫМ ШПИОНАЖЕМ

Задание 1. Система маскировки побочных электромагнитных излучений и наводок Гром ЗИ-4А отличается от аналогичных:

Выберите все правильные ответы (один или несколько)

1) наличием дисконусной антенны;
2) диапазоном рабочих частот;
3) возможностью сопряжения с ПК;
4) наличием ортогональных рамочных антенн.

Задание 2. Основным направлением противодействия утечке информации является обеспечение физической и _____ защиты информационных ресурсов. (вписать пропущенное слово)

Задание 3. Приборы TRN-2000 в составе системы Шторм-7 служат:

Выберите все правильные ответы (один или несколько)

1) для формирования акустических помех;
2) для виброакустической защиты;
3) для формирования помехи в оконных стеклах;
4) для формирования электромагнитных помех в стенах и перекрытиях.

Задание 4. Для обнаружения и локализации радиоизлучающих специальных технических средств может использоваться:

Выберите все правильные ответы (один или несколько)

1) Система «Шторм-7»;
2) Система защиты «Гром ЗИ-4А»;
3) Локатор нелинейностей NJE-4000 (Орион);
4) Детектор поля ST007.

Задание 5. SI-3030, компонент системы Шторм-5, – это:

Выберите все правильные ответы (один или несколько)

1) прибор виброакустической защиты;
2) виброакустический преобразователь;
3) акустический излучатель;
4) электромагнитный излучатель.

Задание 6. Для обнаружения выключенных подслушивающих устройств может использоваться:

Выберите все правильные ответы (один или несколько)

1) Детектор поля ST007;
2) Локатор нелинейностей NJE-4000 (Орион);
3) Многофункциональный поисковый прибор ST-031 «Пиранья».

Задание 7. Использование НЖМД после стирания информации с помощью устройств серии СТЕК-Н проблематично, так как:

Выберите все правильные ответы (один или несколько)

1) стирается служебная информация, записанная на пластинах диска;
2) выполняется низкоуровневое форматирование (low-level formatting) диска;
3) стирается информация, записанная в ПЗУ, что приводит к неработоспособности контроллера НЖМД;
4) разрушается ферромагнитный слой на пластинах НЖМД.

ГЛАВА 51. ПРОГРАММНЫЕ СРЕДСТВА ЗАЩИТЫ. ОБЪЕКТЫ И НАЗНАЧЕНИЕ ПРОГРАММНОЙ ЗАЩИТЫ

Задание 1. Большинство атак на узлы сети реализуется:

Выберите все правильные ответы (один или несколько)

1) по коммутируемым каналам;

2) изнутри корпоративной сети;

3) путем атак на серверы и устройства, установленные внутри DMZ;

4) путем атак межсетевого экрана и вмешательства в трафик, проходящий через него.

Задание 2. Поиск уязвимостей сканерами безопасности основывается:

Выберите все правильные ответы (один или несколько)

1) на попытках имитации проникновения;

2) на использовании базы данных, которая содержит признаки известных уязвимостей;

3) на эвристических методиках, описывающих потенциально опасные для системы действия;

4) на анализе информации о системе (разрешенных протоколах, открытых портах, версиях ПО).

Задание 3. Причиной появления всё новых разновидностей информационных воздействий на сетевые службы, представляющих реальную угрозу защищенности информации, является:

Выберите все правильные ответы (один или несколько)

1) наличие неустранимых уязвимостей в протоколах TCP/IP;

2) высокие темпы развития компьютерной техники, обновления программного обеспечения;

3) повсеместное использование одних и тех же протоколов взаимодействия с Интернетом;

4) верный ответ отсутствует.

ГЛАВА 52. ПОДХОДЫ К ВЫБОРУ СРЕДСТВ ЗАЩИТЫ

Задание 1. Методы сканирования на уровне сети, как правило, не выполняют сканирование:

Выберите все правильные ответы (один или несколько)

1) периметра сети снаружи;
2) внутренней сети со стороны демилитаризованной зоны;
3) при подключении через сервер удаленного доступа;
4) внутренней сети и из внутренней сети.

Задание 2. Ядром системы анализа защищенности на уровне сети является:

Выберите все правильные ответы (один или несколько)

1) база уязвимостей;
2) модуль генерации;
3) модуль сканирования.

Задание 3. Системы анализа защищенности на уровне СУБД чаще всего исполняются _____. (вписать пропущенное слово)

Задание 4. В средствах поиска уязвимостей реализации, как правило, используется:

Выберите все правильные ответы (один или несколько)

1) анализ алгоритма программно-аппаратного обеспечения;
2) анализ проекта системы;
3) анализ на основе исходного текста;
4) анализ на основе исполняемого файла.

Задание 5. Инвентаризацией служб и установленного ПО занимаются:

Выберите все правильные ответы (один или несколько)

1) средства, позволяющие оценить защищенность сети в целом;
2) средства, реализующие основные защитные механизмы;
3) средства непрерывного мониторинга сети и отдельных ее узлов.

Задание 6. Слабости системной политики позволяют выявить средства поиска уязвимостей:

Выберите все правильные ответы (один или несколько)

1) реализации;
2) проектирования;
3) эксплуатации.

Задание 7. По уровню в информационной инфраструктуре наиболее распространенными являются средства анализа защищенности:

Выберите все правильные ответы (один или несколько)

1) на уровне ОС;
2) на уровне СУБД;
3) на уровне приложений;
4) на уровне сети.

Задание 8. К средствам, позволяющим оценить защищенность сети в целом, относятся:

Выберите все правильные ответы (один или несколько)

1) программы, занимающиеся сбором данных;
2) средства обнаружения и противодействия атакам;
3) средства обнаружения уязвимостей.

Задание 9. Системы анализа защищенности на уровне приложений рассчитаны:

Выберите все правильные ответы (один или несколько)

1) только на наиболее популярные приложения;
2) на отслеживание действий любых приложений, ориентируясь на их внешнюю активность;
3) на отслеживание приложений, внесенных в их базы данных.

ГЛАВА 53. ПРОГРАММНАЯ ЗАЩИТА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ. РОЛЕВОЕ УПРАВЛЕНИЕ ДОСТУПОМ В КОММЕРЧЕСКОМ БАНКЕ

Задание 1. RBAC/Web может использоваться с веб-серверами:

Выберите все правильные ответы (один или несколько)

1) только под UNIX;
2) на практически всех операционных системах;
3) только под Windows.

Задание 2. Для безопасной передачи сеансовых ключей («hands-haking») при организации пиринговой сети с криптозащитой применяется:

Выберите все правильные ответы (один или несколько)

1) алгоритм AES;
2) алгоритм 3DES;
3) асимметричный алгоритм шифрования;
4) шифр SEAL.

Задание 3. При использовании объектной технологии для реализации RBAC управление доступом к информации находится исключительно:

Выберите все правильные ответы (один или несколько)

1) в методах класса интерфейса приложения;
2) в ролевых классах;
3) в классе базовых методов доступа.

Задание 4. При статическом распределении обязанностей правила активируются:

Выберите все правильные ответы (один или несколько)

1) при создании роли;
2) при выборе пользователем роли в сеансе работы;
3) при назначении роли администратором.

Задание 5. При использовании RBAC/Web аутентификация пользователя выполняется:

Выберите все правильные ответы (один или несколько)

1) веб-сервером;
2) браузером;
3) средствами RBAC;
4) операционной системой.

Задание 6. В ролевой системе управления доступом роли соответствуют:
Выберите все правильные ответы (один или несколько)

1) операциям, которые должны быть выполнены лицом в отдельной работе;
2) правам и обязанностям пользователя в организации;
3) минимально необходимому уровню доступа к информации для конкретного пользователя.

ЛИТЕРАТУРА

1) Бартош А.А. Основы международной безопасности. Организации обеспечения международной безопасности : учебное пособие для вузов / А.А. Бартош. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 429 с. – (Высшее образование). – ISBN 978-5-534-17521-9. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/540122 (дата обращения: 05.09.2024).

2) Внуков А.А. Защита информации : учебное пособие для вузов / А.А. Внуков. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 161 с. – (Высшее образование). – ISBN 978-5-534-07248-8. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/537247 (дата обращения: 05.09.2024).

3) Зенков А.В. Информационная безопасность и защита информации : учебное пособие для вузов / А.В. Зенков. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 107 с. – (Высшее образование). – ISBN 978-5-534-16388-9. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/530927 (дата обращения: 06.09.2023).

4) Козырь Н.С. Гуманитарные аспекты информационной безопасности : учебное пособие для вузов / Н.С. Козырь, Н.В. Седых. – Москва : Издательство Юрайт, 2024. – 170 с. – (Высшее образование). – ISBN 978-5-534-17153-2. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/544965 (дата обращения: 05.09.2024).

5) Корабельников С.М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С.М. Корабельников. – Москва : Издательство Юрайт, 2024. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/543351 (дата обращения: 05.09.2024).

6) Полякова Т.А. Организационное и правовое обеспечение информационной безопасности : учебник для вузов / Т.А. Полякова, А.А. Стрельцов, С.Г. Чубукова, В.А. Ниесов ; под редакцией Т.А. Поляковой, А.А. Стрельцова. – 2-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2024. – 357 с. – (Высшее образование). – ISBN 978-5-534-19108-0. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/555950 (дата обращения: 05.09.2024).

7) Чернова Е.В. Информационная безопасность человека : учебное пособие для вузов / Е.В. Чернова. – 3-е изд., перераб. и доп. – Москва : Издательство Юрайт, 2023. – 327 с. – (Высшее образование). – ISBN 978-5-534-16772-6. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/531682 (дата обращения: 03.10.2023).

8) Щербак А.В. Информационная безопасность : учебник для среднего профессионального образования / А.В. Щербак. – Москва : Издательство Юрайт, 2023. – 259 с. – (Профессиональное образование). – ISBN 978-5-534-15345-3. – Текст : электронный // Образовательная платформа Юрайт [сайт]. – URL: https://urait.ru/bcode/519614 (дата обращения: 07.09.2023).

КЛЮЧИ К ТЕСТАМ

№ вопроса	Ответ
Глава 1. Национальная и информационная безопасность	
1	Национальные интересы
2	124
3	Национальная безопасность
4	23
5	123
6	4
7	124
8	4
9	123
10	4
11	Информационная безопасность
Глава 2. Понятие информации и обеспечение ее безопасности	
1	2
2	Информация
3	информация
4	Информационная система
5	информационные технологии
Глава 3. Информационные отношения как объект уголовно-правовой охраны и их безопасности	
1	4
2	объектом
3	объектом
4	2
5	Персональные данные
6	123
Глава 4. Информация как предмет уголовно-правовой охраны	
1	4
2	реальной
3	3
4	34
5	предметом
Глава 5. Уголовная ответственность за посягательства на информационную безопасность	
1	2
2	2
3	13
4	4
5	3
6	Специальный
7	Субъективный
8	Семейная
9	1
10	Частная жизнь
11	1
12	3
13	1

14	1
15	прямым
16	3
17	ложные сведения
18	4
19	1
20	1
21	4
22	123
23	2
24	смежным
25	прямым
26	фальсификация
27	прямом
28	клевета
29	4
30	объективный
31	3
32	порочащими
33	заведомо ложной
34	неполной
35	3
36	2
37	принуждение
38	подкуп
39	потерпевшего
40	1
41	Коммерческая тайна
42	Банковская тайна
Глава 6. Обеспечение информационной безопасности в условиях глобализации информационного пространства	
1	Кибербезопасность
2	3
3	Информационная инфраструктура
4	Базы данных
5	123
6	24
7	Духовная культура
8	12
9	2
10	Политическое бытие
11	1
12	Правовой режим
13	23
14	4
15	2
16	134

Глава 7. Теоретические и методологические вопросы организационного и правового обеспечения информационной безопасности	
1	34
2	124
3	123
4	234
5	Интернет
6	23456
7	123
8	Защита
9	4
10	125
11	134
12	234
Глава 8. Организационно-правовые проблемы международной информационной безопасности	
1	2345
2	134
3	информационные ресурсы
4	12456
5	4
Глава 9. Правовые режимы обеспечения безопасности информации ограниченного доступа	
1	2
2	Конфиденциальность
3	Коммерческая тайна
4	3
5	2
6	Допуск
7	Государственная тайна
8	234
9	Тайна
10	Персональные данные
11	124
12	Гриф секретности
13	2
14	134
15	Обработка
Глава 10. Актуальные проблемы правового и организационного обеспечения информационной безопасности	
1	234
2	134
3	123
4	124
5	Блогер
6	Информационный посредник
7	123
8	Информационная продукция

Глава 11. Особенности организационно-правового обеспечения защиты информационных систем	
1	24
2	12
3	Информационная безопасность
4	Политика безопасности – ИТТ
5	Профиль стандартов
6	24
7	124
8	123
Глава 12. Юридическая ответственность за правонарушения в информационной сфере	
1	234
2	14
3	Модификация
4	проступок
5	134
6	234
7	Блокирование
8	23
9	234
10	134
11	123
12	34
13	информационные преступления
Глава 13. Информационное общество	
1	информационные
2	267
3	цивилизации
4	компьютеризации
5	1
6	Первая революция – летопись Вторая революция – печатный станок Третья революция – телеграф Четвертая революция – информационная коммуникация
7	Информационная индустрия
8	достоверной
9	1234
10	Глобализация
11	2
12	качественной и достоверной
13	4
14	дигитизация
15	2
16	1
17	зомбирование
18	3
19	Информационный прессинг
20	дезинформация

Глава 14. Информационно-техническая безопасность	
1	357
2	целостность
3	личная
4	123
5	защита
6	4
7	Нарушитель
8	3
9	123
10	уязвимость
11	4
12	Утрата – потеря или хищение носителя информации, уничтожение носителя информации или информации на нем, модификация или блокирование защищаемой информации. Утечка – неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования. Разглашение – несанкционированное доведение защищаемой информации до неограниченного количества получателей информации.
13	1
14	231
15	2
16	2
17	троянская программа
18	14
Глава 15. Информационно-психологическая безопасность	
1	357
2	целостность
3	личная
4	123
5	защита
6	4
7	Нарушитель
8	3
9	123
10	уязвимость
11	4
12	Утрата – потеря или хищение носителя информации, уничтожение носителя информации или информации на нем, модификация или блокирование защищаемой информации. Утечка – неправомерный выход конфиденциальной информации за пределы защищаемой зоны ее функционирования. Разглашение – несанкционированное доведение защищаемой информации до неограниченного количества получателей информации.
13	1
14	231
15	2
16	2
17	троянская программа
18	14

Глава 16. Информационно-психологическая безопасность в среде информационно-коммуникативных технологий	
1	134
2	MMORPG – разновидность онлайновых ролевых игр, позволяющая множеству людей одновременно играть в изменяющемся виртуальном мире через Интернет. E-mail – система пересылки почтовых сообщений между абонентами. Форум – организация обмена информацией и общения между большим количеством собеседников, которым небезынтересна тема обсуждения, которая и является причиной концентрации этих людей в одном месте для вынесения её на всеобщее обсуждение. Чат – средство общения пользователей по сети в режиме реального времени, а также программное обеспечение, позволяющее организовывать такое общение.
3	4
4	4
5	1
6	3
7	1
8	2
9	Черный список
10	1
11	3
12	Этика – наука, изучающая мораль, нравственность как форму общественного сознания и как вид общественных отношений. Этикет – правила хорошего тона, принятые в социальной группе. Нетикет – правила поведения, общения в сети Интернет. Компьютерная этика – нормы поведения в сетевой среде.
13	1
14	124
15	2
16	3
17	1
18	девиантного
Глава 17. Введение в информационную безопасность	
1	4
2	2
3	4
4	4
5	2
6	3
7	1
8	1
9	4
Глава 18. Угрозы	
1	4
2	3
3	2
4	4
5	1
6	4

7	2
8	4
9	1
10	2
11	4
Глава 19. Проблемы безопасности интернет-протоколов	
1	3
2	логическими
3	3
4	DHCP
5	NAT-бокс
6	2
7	2
8	1
9	1
10	2
11	4
12	4
13	3
14	2
15	2
Глава 20. Построение системы безопасности	
1	4
2	3
3	2
4	3
5	1
6	2
7	2
8	3
9	3
10	4
Глава 21. Критерии оценки	
1	Четыре группы
2	1
3	2
4	1
5	7 ступеней
6	3
7	3
8	1
9	4
Глава 22. Модели безопасности	
1	2
2	3
3	1
4	4
5	Гибкая
6	4
7	3
8	2

9	3
10	2
Глава 23. Технологии работы с ключами	
1	1
2	3
3	2
4	Длиннее
5	1
6	1
7	2
8	4
Глава 24. Технологии работы с ключами	
1	3
2	1
3	2
4	2
5	2
6	2
7	2
Глава 25. Аутентификация на основе обладания предметом	
1	2
2	12
3	1
4	23
5	2
6	Загрузки
7	4
8	3
9	2
10	4
11	3
Глава 26. Биометрическая аутентификация	
1	1
2	4
3	3
4	1
5	3
6	2
7	3
8	1
Глава 27. Особенности аутентификации в распределенных системах	
1	1
2	3
3	4
4	Майнингом
5	3
6	1
Глава 28. Основы криптографической защиты информации	
1	4
2	3

3	32!
4	4
5	3
6	2
7	1
8	4
9	3
10	4
11	4
12	4
13	3
14	1
15	2
16	3
17	3
18	4
19	2
20	4
Глава 29. Современные криптографические алгоритмы	
1	3
2	1
3	3
4	12
5	2
6	2
7	3
8	4
9	3
Глава 30. Электронная цифровая подпись	
1	4
2	2
3	3
4	2
5	12
6	3
7	1
8	1
9	1
10	4
Глава 31. Безопасность сетей	
1	1
2	4
3	2
4	2
Глава 32. Безопасность мобильной и беспроводной связи	
1	2
2	4
3	2
4	1
5	1

6	2
7	3
8	2
9	2
Глава 33. Инженерно-техническая защита информации	
1	2
2	3
3	2
4	4
5	1
6	3
Глава 34. Правовые основы информационной безопасности	
1	2
2	4
3	1
4	1
5	1
6	1
7	3
8	1
Глава 35. Управление IT-проектом как эффективный способ организации действий по повышению уровня информационной безопасности	
1	123
2	2
3	1
4	1
Глава 36. Основные определения	
1	Целостность данных
2	3
3	4
4	1
5	2
Глава 37. Правовые аспекты информационной безопасности и защиты информации	
1	5
2	2,3
3	4
4	4
5	2,4
6	4
7	4
8	1,5
Глава 38. Материалы к практическим занятиям: элементы теории чисел	
1	факторизацией
2	криптология
3	3
4	2
5	шифрование

Глава 39. Сетевое взаимодействие и информационная безопасность современного общества	
1	2
2	4
3	3
4	1
5	4
6	4
7	1
8	4
9	3
10	3
11	3
12	4
13	2
14	1
15	3
Глава 40. Социальная инженерия как основная угроза информационной безопасности общества	
1	2
2	1
3	4
4	3
5	1
6	3
7	4
8	4
9	1
10	4
11	4
12	4
13	4
14	2
15	4
16	4
17	4
18	2
19	1
20	3
Глава 41. Цифровизация общества: предпосылки, тенденции, перспективы	
1	1
2	4
3	4
4	1
5	2
6	4
7	4
8	2
9	4
10	1

11	2
12	4
13	3
14	4
15	4
16	2
17	2
18	1
19	4
Глава 42. Нормативно-правовое регулирование и обеспечении информационной безопасности общества	
1	2
2	4
3	2
4	2
5	4
6	1
7	1
8	4
9	3
10	3
11	4
12	1
13	1
14	3
15	1
Глава 43. Международная безопасность как сфера мирового взаимодействия	
1	1,3,4,5
2	Коллективная безопасность
3	3
4	4
5	Международная безопасность
6	3,4,6
7	1
8	2
9	2,3,6
10	2
11	Глобальное управление
12	1,2,5
13	Политический риск
14	3
15	Стратегия измора
Глава 44. Организации обеспечения международной безопасности в многополярном мире	
1	4
2	1,2,7,8,9
3	1
4	1,2,4
5	1
6	2
7	3

8	1,2,4,5
9	2
10	1
11	1,2,4
12	2,3,4,5
13	2,3,4,5,6,7
14	3,4,5,6,7,8
15	1
16	1,2,3,4,5
17	2
18	3
19	3
20	2
21	1,2,3,4
Глава 45. НАТО	
1	1,2,3,4,6
2	3
3	4
4	4
5	4
6	1,3,5
7	3
8	1
9	3
10	1,3,4
11	1
12	1
13	1,2,4,5,6
14	1
15	2
16	1
17	2,3,4
Глава 46. Модели и механизмы мирового политического развития	
1	1,2,3,4,5
2	1,2,3,4
3	4
4	1-г, 2-б, 3-в, 4-а
5	1,2,3,4
6	2,3,4,5
7	Модель
8	4
9	1,2,4
10	1,2,3,4,5,6
11	Самоограничение
12	2
13	1,2,3,4,5,6
14	4

Глава 47. Авторское право. Охрана авторского права государством	
1	3
2	2,3,4
3	2
4	1,2,3
5	2
6	Следования
7	3
8	2
9	3
Глава 48. Роли и обязанности должностных лиц по разработке и внедрению политики безопасности	
1	3
2	3
3	Целостности
4	4
5	2
6	2
Глава 49. Каналы утечки информации	
1	1
2	1
3	1,2
4	2
5	3
6	2,4
Глава 50. Технические средства борьбы с промышленным шпионажем	
1	1
2	Логической
3	4
4	4
5	1
6	2
7	1
Глава 51. Программные средства защиты. Объекты и назначение программной защиты	
1	2
2	2
3	1
Глава 52. Подходы к выбору средств защиты	
1	3
2	3
3	Удаленно
4	4
5	3
6	3
7	4
8	3
9	1

Глава 53. Программная защита интеллектуальной собственности. Ролевое управление доступом в коммерческом банке	
1	2
2	3
3	3
4	3
5	1
6	2

ОПИСАНИЕ ФУНКЦИОНАЛЬНОСТИ ИЗДАНИЯ:

Электронное издание имеет интерактивное содержание, позволяющее переходить к тексту по щелчку компьютерной мыши.

МИНИМАЛЬНЫЕ СИСТЕМНЫЕ ТРЕБОВАНИЯ:

Минимальные системные требования: Celeron 1600 Mhz; 128 Мб RAM; Windows XP/7/8 и выше; 8x CD-ROM; разрешение экрана 1024×768 или выше; программа для просмотра pdf.

СВЕДЕНИЯ О ЛИЦАХ, ОСУЩЕСТВЛЯВШИХ ТЕХНИЧЕСКУЮ ОБРАБОТКУ И ПОДГОТОВКУ МАТЕРИАЛОВ:

Оформление электронного издания : Издательский центр «Удмуртский университет».

Компьютерная верстка: Т.В. Опарина

Авторская редакция

Подписано к использованию 11.09.2025
Объем электронного издания 2,1 Мб, тираж 10 экз.
Издательский центр «Удмуртский университет»
426034, г. Ижевск, ул. Ломоносова, д. 4Б, каб. 021
Тел. : +7(3412)916-364 E-mail: editorial@udsu.ru