МИНОБРНАУКИ РОССИИ
Юго-Западный государственный университет

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

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

Работа с конфиденциальной информацией
(наименование учебной дисциплины)

10.03.01 Информационная безопасность, профиль «Безопасность автоматизированных систем в сфере информационных и коммуникационных технологий»
(код и наименование ОПОП ВО)

Курск – 2022

1 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

1.1 ВОПРОСЫ ДЛЯ СОБЕСЕДОВАНИЯ.

Тема 1. Организационные и правовые основы обеспечения безопасности конфиденциальной информации

1. Какие существуют правовые нормы в области защиты информации?
2. Что регулирует Концепция национальной безопасности Российской Федерации?
3. Что представляет собой система безопасности?
4. Что такое «организационная защита информации»?
5. Какие есть требования к построению систем безопасности предприятия и учреждения?
6. Какова общая характеристика организационных методов обеспечения

безопасности конфиденциальной информации?

Тема 2. Организационные источники и каналы утечки информации

1. Что такое защитные действия?
2. По какому основанию классифицируются защитные действия?
3. Что следует сделать для того, чтобы исключить неправомерное овладение конфиденциальной информацией?
4. Что является основными целями защиты информации в информационных системах?
5. Что представляет собой разглашение защищаемой информации?
6. В каких случаях возможно разглашение конфиденциальной информации?

Тема 3. Технические и программные средства защиты информации

1. Как выглядит системная классификация технических средств защиты?
2. Какие существуют средства поиска закладных устройств?
3. Какими пользуются средства нейтрализации технических каналов утечки информации (ТКУИ)?
4. Перечислите технические средства идентификации и установления подлинности?
5. Какие есть основные программные средства защиты ПЭВМ от НСД?
6. Что представляют собой технические средства защиты?

Тема 4. Коммерческая тайна и порядок ее определения

1. Какие существуют основные понятия, относящиеся к коммерческой тайне?

2. Какие действия со сведениями относятся к коммерческой конфиденциальности информации?
3. Какова будет ответственность за нарушение коммерческой тайны?
4. Для чего введен Федеральный закон № 98-ФЗ «О коммерческой тайне»?
5. Что регулирует Закон от 29.07.2004 «О коммерческой тайне»?
6. Что понимают под «коммерческой тайной»?

Тема 5. Организация работ с информацией, составляющей коммерческую тайну

1. Какова ответственность за нарушение Федерального закона № 98-ФЗ «О коммерческой тайне»?
2. Что могут предоставлять руководители среднего звена управления фирмой в пределах разрешительной системы?
3. Что необходимо указать в Положении о разрешительной системе фирмы?
4. Как происходит допуск сотрудников к работе с документами, имеющими гриф "КТ"?
5. Соблюдение каких правил необходимо для эффективной работы разрешительной системы?
6. Какие лица допускаются к сведениям, составляющим коммерческую тайну?

Тема 6. Подбор персонала на должности, связанные с работой с информацией ограниченного доступа

1. Как рассматривается персонал организации как источник информации и один из основных каналов ее разглашения?
2. С помощью каких способов происходит разглашение информации?
3. В каких случаях возможно разглашение конфиденциальной информации?
4. Как классифицируются каналы распространения информации?
5. Что лежит в основе защиты информации от разглашения?
6. Каков порядок профотбора персонала на предприятие?

Тема 7. Организация деятельности службы безопасности объекта

1. Каковы задачи службы безопасности организации?
2. Какова организационная структура службы безопасности?
3. Какие функции службы безопасности?
4. Какие есть структурные подразделения службы безопасности?
5. Чем характеризуется служба безопасности предприятия?
6. Для чего необходим отдел защиты информации?

Тема 8. Организация внутриобъектового режима

1. Каковы основные задачи организации внутриобъектового режима?

2. Как происходит организация охраны объектов на территории предприятия?
3. Для чего необходима организация инженерно-технической безопасности?
4. Как осуществляется организация безопасности информационных систем?
5. Что представляет собой «внутриобъектовный режим»?
6. Какие существуют виды охраны, согласно классификации?

Тема 9. Требования, предъявляемые к помещениям и хранилищам, в которых ведутся закрытые работы, хранятся документы ограниченного доступа и изделия

1. Для чего необходимо ограждение периметра, отдельных участков территории объекта?
2. Что представляет собой контрольно-пропускной пункт объекта?
3. Для чего предназначена техническая укрепленность строительных конструкций зданий и помещений?
4. Как осуществляется защита периметра территории зданий и открытых площадок с помощью технических средств охраны?
5. Что представляет защита помещений объекта с помощью технических средств охраны?
6. Что включает защита персонала и посетителей объекта?

Тема 10. Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей

1. Как следует проводить организацию приема посетителей в организации?
2. Какая существует классификация посетителей организации?
3. Какие могут быть угрозы информационной безопасности, исходящие от посетителей?
4. Какие существуют правила при приеме руководителем фирмы (предприятия) и руководящим составом различных категорий посетителей?
5. Как проводится работа с иностранными представителями?
6. Что входит в программу приема делегации специалистов?

Тема 11. Организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа.

1. Какие существуют основные понятия, связанные со служебным расследованием?
2. Дайте основание для проведения служебного расследования?
3. Каковы цели служебного расследования?

4. Каковы задачи служебного расследования по фактам разглашения информации ограниченного доступа?
5. Каково содержание заключения служебного расследования?
6. Каков порядок проведения проверки наличия документов, дел и носителей информации ограниченного доступа?

Тема 12. Охрана объектов

1. Какие цели преследует охрана объектов?
2. Каковы задачи охраны объектов?
3. Что представляют собой объекты охраны?
4. Какие существуют виды и способы охраны?
5. Как взаимодействует посты охраны с местными органами правопорядка?
6. Как происходит прием и сдача объекта под охрану?

Тема 13. Организация защиты информации при подготовке и проведению совещаний и переговоров

1. Каковы основные причины, по которым информация может разглашаться на конфиденциальных совещаниях или переговорах?
2. На каких этапах проводятся конфиденциальные совещания и переговоры?
3. Какие документы составляют при подготовке конфиденциального совещания?
4. Каков порядок подготовки конфиденциального совещания?
5. Какие обязанности у сотрудников службы безопасности при подготовке совещаний и переговоров?
6. Что понимается под разглашением (оглаской, оглашением) конфиденциальной информации?

Тема 14. Организация защиты информации при осуществлении научно-публицистической деятельности

1. Что является источниками ценных сведений в процессе выставочной деятельности?
2. Как обеспечивается безопасность конфиденциальной информации в рекламно-выставочных материалах?
3. Где обычно проводятся переговоры?
4. Как организуется защита информации в рекламно-выставочной деятельности?
5. Что необходимо сделать для обеспечения безопасности конфиденциальной информации в рекламно-выставочных материалах?
6. Что входит в понятие научно-публицистической деятельности?

Тема 15. Защита информации при рекламной деятельности

1. Что регулируется Федеральным Законом «О рекламе»?

2. Что включают в себя рекламно-выставочные материалы?
3. Как происходит защита информации в рекламно-выставочной деятельности?
4. Для обеспечения безопасности конфиденциальной информации в рекламно-выставочных материалах следует?
5. Основными направлениями защиты информации в рекламной деятельности являются?
6. Дайте определение рекламе и рекламной деятельности.

Тема 16. Основные принципы организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации

1. Дайте понятие информационно-аналитической работы?
2. Какие основные задачи решает информационно-аналитическое подразделение службы безопасности?
3. Какие осуществляет функции информационно-аналитическое подразделение службы безопасности?
4. Каковы направления аналитической работы ИАС?
5. Как происходит аналитическая работа с источниками угрозы конфиденциальной информации?
6. Чем представлена аналитическая работа в деятельности организаций и фирм?

Тема 17. Подготовка лиц, ответственных за обеспечение безопасности информации

1. Как происходит выбор и подготовка персонала к работе, связанной с секретами фирмы?
2. Охарактеризуйте особенности обучения персонала правилам защиты информации?
3. Какие необходимы организационные мероприятия по работе с персоналом, получившим доступ к конфиденциальной информации?
4. Для чего предназначена эксплуатация систем защиты информации?
5. Как производится оценка профессиональных способностей сотрудников, связанных с секретами фирмы?
6. Какие организационные мероприятия необходимы для работы с персоналом, получившим доступ к конфиденциальной информации?

Тема 18. Содержание основных методов и работы с персоналом, обладающим конфиденциальной информацией

1. Что представляет собой анализ информации?
2. Как происходит установление личности нарушителя режима коммерческой тайны?
3. Какие принимаются меры предупреждения обстоятельств организационно-управленческого, воспитательного и правового характера?

4. Как происходит обеспечение защищающими и использующими информацию ограничительного характера?
5. Для чего проводится анализ основных методов получения конфиденциальной информации у персонала?
6. Какая работа проводится с персоналом, владеющим конфиденциальной информацией?

Критерии оценки:

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

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

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

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

1.2 КОНТРОЛЬНЫЕ ВОПРОСЫ ДЛЯ ЗАЩИТЫ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа №1. «Законодательство об информационной безопасности»

1. Какие существуют правовые методы защиты в нормативных актах других отраслей законодательства?
2. Что регулирует законодательство о защите государственной тайны?
3. Что регулирует законодательство о защите коммерческой тайны и других негосударственных видов тайны?
4. Как действует законодательство о защите персональных данных?
5. Перечислите организационные документы системы защиты информации?
6. Какие вы знаете технологические документы системы защиты информации?
7. Чем представлена регламентация системы защиты информации для условий экстремальных ситуаций?

Практическая работа №2. «Организационные источники и каналы утечки информации»

1. Какие есть источники информации?
2. С какими угрозами сталкивается конфиденциальная информация?
3. Какие средства применяются для организационной защиты информации?
4. С помощью каких условий можно достичь организационной защиты информации?
5. Какие каналы могут использоваться для распространения информации?
6. Как происходит утечка информации?
7. Какие каналы передают информацию?

Практическая работа №3. «Технические средства защиты информации»

1. Какие используют программные средства защиты информации?
2. Что представляют собой «программные средства защиты информации»?
3. Какие существуют технические средства защиты информации?
4. Какие вы знаете программные средства защиты информации?
5. Что представляют собой «технические средства защиты информации»?
6. Что такое «средства защиты информации»?

Практическая работа №4. «Коммерческая тайна и порядок ее определения»

1. Что такое «коммерческая тайна»?

2. У кого есть допуск к конфиденциальной информации и документам, составляющим коммерческую тайну?

3. Какова цель информационных ресурсов в предпринимательской сфере?

4. Как происходит организация работ с информацией, составляющей коммерческую тайну?

5. Каков порядок определения коммерческой тайны?

6. Какие стоят задачи у информационных ресурсов в предпринимательской сфере?

7. Какие есть направления классификации информационных ресурсов в предпринимательской сфере?

Практическая работа №5. «Организация внутриобъектового режима»

1. Как происходит организация деятельности службы безопасности объекта?
2. Какие задачи стоят перед службой безопасности организации?
3. В чем особенности методического подхода к формированию структуры службы безопасности?
4. Какова организационная структура службы безопасности?
5. Каковы функции службы безопасности?

6. Укажите, какие основные документы регламентируют деятельность службы безопасности объекта?

7. Какие есть особенности действий сотрудников службы безопасности в чрезвычайных ситуациях и в условиях чрезвычайного положения?

Практическая работа №6. «Организация защиты информации при приеме в организации посетителей командированных лиц и иностранных представителей»

1. Как происходит организация приема посетителей в организации?

2. По каким критериям основана классификация посетителей?

3. Какие существуют угрозы информационной безопасности, исходящие от посетителей?

4. Какие правила необходимо соблюдать при приеме руководителем фирмы (предприятия) и руководящим составом различных категорий посетителей?

5. Как осуществляется организация проведения служебного расследования по фактам разглашения сотрудниками информации ограниченного доступа?

6. Какие правила необходимо соблюдать при приеме иностранных представителей?

Практическая работа №7. «Организация охраны объекта»

1. На какие виды делятся посты охраны и связь?
2. Как происходит взаимодействие с местными органами правопорядка?

3. Какие существуют способы охраны объекта?
4. Для чего применяют собак в борьбе с нарушителями?
5. Как ведется прием и сдача объекта под охрану?
6. Какие существуют средства и методы физической защиты объектов?
7. Какие используются технические средства охраны и видеонаблюдения объекта?

Практическая работа №8. «Организация защиты информации при подготовке и проведении совещаний и переговоров. Организация защиты информации при осуществлении научно-публицистической и рекламной деятельности»

1. Какие документы составляются при подготовке конфиденциального совещания?
2. Каков порядок подготовки конфиденциального совещания?
3. Какие имеются обязанности у сотрудников службы безопасности при проведении переговоров?
3. Какие проходят этапы при проведении конфиденциальных совещаний и переговоров?
4. На каком основании производится доступ участников на конфиденциальное совещание?
5. Какие требования предъявляются к участникам конфиденциального совещания?
6. Как происходит обеспечение защиты информации при осуществлении закрытой и открытой публикации и рекламной деятельности?
7. Как происходит сбор информации силами предприятия и с привлечением сторонних фирм?

Практическая работа №9. «Организация аналитической работы по предупреждению утечки конфиденциальной информации. Методы работы с персоналом, конфиденциальной информацией»

1. Какими пользуются основными принципами организации аналитической работы служб безопасности по недопущению утечки конфиденциальной информации?
2. Какие методы используются аналитическими подразделениями служб безопасности, по предупреждению утечки конфиденциальной информации?
3. Что представляет собой «оценка профессиональных способностей сотрудников, связанных с секретами фирмы»?
4. Какие проводятся организационные мероприятия по работе с персоналом, получившим доступ к конфиденциальной информации и эксплуатации систем защиты информации;
5. Какие проводятся организационные мероприятия по эксплуатации систем защиты информации?

6. Какие существуют особенности приема и перевода сотрудников на работу, связанную с владением конфиденциальной информацией?
7. Что представляет собой текущая работа с персоналом, владеющим конфиденциальной информацией?

Критерии оценки:

6-5 баллов (или оценка «отлично») выставляется обучающемуся, если он демонстрирует глубокое знание содержания вопроса; дает точные определения основных понятий; аргументированно и логически стройно излагает учебный материал; иллюстрирует свой ответ актуальными примерами (типовыми и нестандартными), в том числе самостоятельно найденными; не нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

4-3 балла (или оценка «хорошо») выставляется обучающемуся, если он владеет содержанием вопроса, но допускает некоторые недочеты при ответе; допускает незначительные неточности при определении основных понятий; недостаточно аргументированно и (или) логически стройно излагает учебный материал; иллюстрирует свой ответ типовыми примерами.

2-1 балла (или оценка «удовлетворительно») выставляется обучающемуся, если он освоил основные положения контролируемой темы, но недостаточно четко дает определение основных понятий и дефиниций; затрудняется при ответах на дополнительные вопросы; приводит недостаточное количество примеров для иллюстрирования своего ответа; нуждается в уточняющих и (или) дополнительных вопросах преподавателя.

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ

2.1 БАНК ВОПРОСОВ И ЗАДАНИЙ В ТЕСТОВОЙ ФОРМЕ

Задания в закрытой форме

1. Кто отвечает за учет, хранение и использование документов, содержащих конфиденциальные сведения:

(1) секретарь

(2) любой сотрудник

(3) должностное лицо, назначенное приказом руководителя

2. Какие сведения указываются на последнем листе документа:

(1) гриф ограничения доступа к документу

(2) фамилия и номер телефона исполнителя

(3) фамилии должностных лиц, имеющих доступ к документу

3. Печатание конфиденциальных документов производится:

(1) сотрудником машбюро

(2) сотрудником службы конфиденциальной информации

(3) исполнителем

4. При изготовлении документов, содержащих конфиденциальную информацию, не должны использоваться:

(1) новая красящая лента

(2) бумага хорошего качества

(3) копировальная бумага

(4) новая копировальная бумага

5. Ставится ли гриф конфиденциальности на конверте:

(1) да

(2) нет

6. Прием и предварительное рассмотрение документов, содержащих конфиденциальные сведения, осуществляются:

(1) секретарем

(2) сотрудником службы конфиденциальной информации

(3) сотрудником, назначенным руководителем

7. Может ли с документа, поступившего с грифом ограниченного доступа, этот гриф снят:

(1) да, если документ не входит в Перечень документов фирмы, отнесенных к категории конфиденциальных

(2) нет, если документ входит в Перечень

(3) нет, если документ не входит в Перечень

8. Отправка конфиденциальных документов осуществляется:

(1) секретарем

(2) исполнителем

(3) сотрудником службы конфиденциальной информации

9. Документы, содержащие конфиденциальную информацию, регистрируются:

(1) вместе с другими документами

(2) отдельно от остальной корреспонденции

(3) на персональном компьютере

10. Номенклатура дел для документов, содержащих гриф «КТ», является:

(1) составной частью общей номенклатуры дел

(2) самостоятельным документом

(3) общей номенклатурой, но на делах с конфиденциальными документами ставится особая отметка

11. Документы, имеющие гриф «КТ», формируются:

(1) в отдельное дело (дела)

(2) в те же дела, что и открытые документы

12. Список сотрудников, имеющих право пользоваться делом, пишется:

(1) на обложке дела

(2) на внутренней стороне обложки дела

(3) в описи дела

(4) в заверительном листе к делу

13. Назовите разделы номенклатуры дел:

(1) индекс дела

(2) гриф конфиденциальности

(3) заголовок дела

(4) фамилия и инициалы лиц, которым предоставляется право пользования делом;

(5) номер тома;

(6) дата

(7) количество листов в томе

(8) дата заведения и закрытия дела

(9) срок хранения и номер статьи Перечня

(10) архивный шифр, номер акта об уничтожении

14. С какими документами должен познакомиться работник, получивший доступ к конфиденциальной информации:

(1) обязательство о неразглашении коммерческой тайны

(2) должностная инструкция

(3) памятка работнику

(4) примерный перечень сведений, составляющих коммерческую тайну

15. Коммерческий документ, представляющий собой претензии к стороне, нарушившей принятые по договору обязательства, и требование возмещения убытков, называется:

(1) исковое заявление

(2) рекламация

(3) протокол разногласий

16. Ответ на претензию предъявляется:

(1) в письменном виде

(2) в устной форме

17. Информация это:

(1) сведения, поступающие от СМИ

(2) только документированные сведения о лицах, предметах, фактах, событиях

(3) сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

(4) только сведения, содержащиеся в электронных базах данных

18. Информация:

(1) не исчезает при потреблении

(2) становится доступной, если она содержится на материальном носителе

(3) подвергается только «моральному износу»

(4) характеризуется всеми перечисленными свойствами

19. Информация, зафиксированная на материальном носителе, с реквизитами:

(1) позволяющими ее идентифицировать, называется

(2) достоверной

(3) конфиденциальной

(4) документированной

(5) коммерческой тайной

20. Формы защиты интеллектуальной собственности:

(1) авторское, патентное право и коммерческая тайна

(2) интеллектуальное право и смежные права

(3) коммерческая и государственная тайна

(4) гражданское и административное право

21. По принадлежности информационные ресурсы подразделяются на:

(1) государственные, коммерческие и личные

(2) государственные, не государственные и информацию о гражданах

(3) информацию юридических и физических лиц

(4) официальные, гражданские и коммерческие

22. К негосударственным относятся информационные ресурсы:

(1) созданные, приобретенные за счет негосударственных учреждений и организаций

(2) созданные, приобретенные за счет негосударственных предприятий и физических лиц

(3) полученные в результате дарения юридическими или физическими лицами

(4) указанные в п.1-3

23. По доступности информация классифицируется на:

(1) открытую информацию и государственную тайну

(2) конфиденциальную информацию и информацию свободного доступа

(3) информацию с ограниченным доступом и общедоступную информацию

(4) виды информации, указанные в остальных пунктах

24. К конфиденциальной информации относятся документы, содержащие:

(1) государственную тайну

(2) законодательные акты

(3) «ноу-хау»

(4) сведения о золотом запасе страны

25. Запрещено относить к информации ограниченного доступа:

(1) информацию о чрезвычайных ситуациях

(2) информацию о деятельности органов государственной власти

(3) документы открытых архивов и библиотек

(4) все, перечисленное в остальных пунктах

26. К конфиденциальной информации не относится:

(1) коммерческая тайна

(2) персональные данные о гражданах

(3) государственная тайна

(4) «ноу-хау»

27. Вопросы информационного обмена регулируются правом:

(1) гражданским

(2) информационным

(3) конституционным

(4) уголовным

28. Согласно ст.132 ГК РФ интеллектуальная собственность это:

(1) информация, полученная в результате интеллектуальной деятельности индивида

(2) литературные, художественные и научные произведения

(3) изобретения, открытия, промышленные образцы и товарные знаки

(4) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

29. Интеллектуальная собственность включает права, относящиеся к:

(1) литературным, художественным и научным произведениям, изобретениям и открытиям

(2) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам

(3) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям

= всему, указанному в остальных пунктах

30. Конфиденциальная информация это:

(1) сведения, составляющие государственную тайну

(2) сведения о состоянии здоровья высших должностных лиц

(3) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ

(4) данные о состоянии преступности в стране

31. Какая информация подлежит защите:

(1) информация, циркулирующая в системах и сетях связи

(2) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

(3) только информация, составляющая государственные информационные ресурсы

(4) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

32. Система защиты государственных секретов определяется Законом:

(1) «Об информации, информатизации и защите информации»

(2) «Об органах ФСБ»

(3) «О государственной тайне»

(4) «О безопасности»

33. Государственные информационные ресурсы не могут принадлежать:

(1) физическим лицам

(2) коммерческим предприятиям

(3) негосударственным учреждениям

(4) всем перечисленным субъектам

34. Из нижеперечисленных законодательных актов наибольшей юридической силой в вопросах информационного права обладает:

(1) Указ Президента «Об утверждении перечня сведений, относящихся к государственной тайне»

(2) Гражданский Кодекс РФ

(3) Закон «Об информации, информатизации и защите информации»

(4) Конституция РФ

35. Классификация и виды информационных ресурсов определены:

(1) Законом «Об информации, информатизации и защите информации»

(2) Гражданским кодексом РФ

(3) Конституцией РФ

(4) всеми документами, перечисленными в остальных пунктах

36. Определение понятия «конфиденциальная информация» дано в:

(1) Гражданский Кодекс РФ

(2) Законе «О государственной тайне»

(3) Законе «Об информации, информатизации и защите информации»

(4) Уголовный Кодекс РФ

37. Формой правовой защиты литературных, художественных и научных произведений является право:

(1) литературное

(2) художественное

(3) авторское

(4) патентное

38. Запрещено относить к информации с ограниченным доступом:

(1) законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны)

(2) только информацию о чрезвычайных ситуациях

(3) только информацию о деятельности органов государственной власти, кроме государственной тайны

(4) документы всех библиотек и архивов

39. Формой правовой защиты изобретений является:

(1) институт коммерческой тайны

(2) патентное право

(3) авторское право

(4) все, перечисленное в остальных пунктах

40. К коммерческой тайне могут быть отнесены:

(1) сведения не являющиеся государственными секретами

(2) сведения, связанные с производством и технологической информацией

(3) сведения, связанные с управлением и финансами

(4) сведения, перечисленные в остальных пунктах

41. Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности:

(1) да

(2) нет

(3) только авторское и патентное

(4) только КТ

42. «Ноу-хау» это:

(1) незащищенные новшества

(2) защищенные новшества

(3) общеизвестные новые технологии

(4) опубликованные технические и технологические новинки

43. Каким законом в РФ защищаются права исполнителей и производителей фонограмм:

(1) «О правовой охране программ для ЭВМ и баз данных»

(2) «Об авторском праве и смежных правах»

(3) «Патентный закон РФ»

(4) закон еще не принят

44. Закон «Об авторском праве и смежных правах» защищает права:

(1) исполнителей (актеров, певцов и т.д.)

(2) производителей фонограмм

(3) организации эфирного и кабельного вещания

(4) всех лиц, перечисленных в остальных пунктах

45. Какой законодательный акт содержит сведения по защите коммерческой тайны:

(1) Закон «Об авторском праве и смежных правах»

(2) Закон «О коммерческой тайне»

(3) Патентный закон

(4) Закон «О правовой охране программ для ЭВМ и баз данных»

46. К информации ограниченного доступа не относится:

(1) государственная тайна

(2) размер золотого запаса страны

(3) персональные данные

(4) коммерческая тайна

47. Система защиты государственных секретов:

(1) основывается на Уголовном Кодексе РФ

(2) регулируется секретными нормативными документами

(3) определена Законом РФ «О государственной тайне»

(4) осуществляется в соответствии с п.1-3

48. Действие Закона «О государственной тайне» распространяется:

(1) на всех граждан и должностных лиц РФ

(2) только на должностных лиц

(3) на граждан, которые взяли на себя обязательство выполнять требования

(4) законодательства о государственной тайне

(5) на всех граждан и должностных лиц, если им предоставили для работы закрытые сведения

49. К государственной тайне относится:

(1) информация в военной области

(2) информация о внешнеполитической и внешнеэкономической деятельности государства

(3) информация в области экономики, науки и техники и сведения в области разведывательной и оперативно-розыскной деятельности

(4) все выше перечисленное

50. Документы, содержащие государственную тайну снабжаются грифом:

(1) «секретно»

(2) «совершенно секретно»

(3) «особой важности»

(4) указанным в п.1-3

51. Гриф «ДСП» используется:

(1) для секретных документов

(2) для документов, содержащих коммерческую тайну

(3) как промежуточный для несекретных документов

(4) в учебных целях

52. Порядок засекречивания состоит в установлении следующих принципов:

(1) целесообразности и объективности

(2) необходимости и обязательности

(3) законности, обоснованности и своевременности

(4) всех выше перечисленных

53. Предельный срок пересмотра ранее установленных грифов секретности составляет:

(1) 5 лет

(2) 1 год

(3) 10 лет

(4) 15 лет

54. Срок засекречивания сведений, составляющих государственную тайну:

(1) составляет 10 лет

(2) ограничен 30 годами

55. Что не относится к общедоступной информации:

(1) информация о состоянии окружающей среды

(2) информация из библиотек, музеев и архивов

(3) информация о полномочиях органов власти

(4) информация о дислокации режимных объектов

56. Какие сведения могут относиться к государственной тайне:

(1) сведения в области контрразведки

(2) сведения в области внешней политики и экономики

(3) сведения в области охраны здоровья нации

(4) только первый и второй пункты

57. Какой профессиональной тайны не существует:

(1) тайны работника социальной службы

(2) тайны почтовых отправлений

(3) тайны работника промышленных объектов

(4) нотариальной тайны

58. В каком случае журналисты могут использовать информацию о частной жизни людей:

(1) при наличии государственных, общественных и иных публичных интересов

(2) в случаях, когда информация о частной жизни человека ранее стала общедоступной

(3) если информация о частной жизни раскрыта самим гражданином или по его воле

(4) во всех трех случаях

59. В каких случаях для использования персональных данных надо получить обязательное согласие человека:

(1) если осуществляется использование общедоступных персональных данных

(2) если публикуются данные из деклараций чиновников

(3) если персональные данные журналисту передал работодатель субъекта персональных данных

(4) если персональные данные публикуются ради общественного интереса

60. Что относится к коммерческой тайне предприятия:

(1) сведения о задолженности работодателей по выплате заработной платы и социальным выплатам

(2) ведения о результатах интеллектуальной деятельности в научно-технической сфере

(3) сведения о показателях травматизма на производстве

(4) сведения о перечне лиц, имеющих право действовать без доверенности от имени юридического лица

61. Какая информация не может быть ограничена в доступе со ссылкой на то, что она является служебной:

(1) нормативные правовые акты, затрагивающие права, свободы и обязанности человека и гражданина

(2) сведения о структуре органа исполнительной власти, его функциях, направлениях и формах деятельности

(3) порядок рассмотрения и разрешения заявлений и обращений граждан, а также юр. лиц и принятых по ним решений

(4) все три пункта

62. Режим защиты информации не устанавливается в отношении сведений, относящихся к:

(1) государственной тайне

(2) деятельности государственных деятелей

(3) конфиденциальной информации

(4) персональным данным

63. Засекречиванию подлежат сведения о:

(1) состоянии демографии

(2) состоянии преступности

(3) фактах нарушения прав и свобод человека и гражданина

(4) силах и средствах гражданской обороны

64. Режим документированной информации – это:

(1) выделенная информация по определенной цели

(2) электронный документ с электронно-цифровой подписью

(3) выделенная информация в любой знаковой форме

(4) электронная информация, позволяющая ее идентифицировать

65. Режим общественного достояния устанавливается для:

(1) любой общедоступной информации

(2) сведений, которые являются уникальными, незаменимыми по своей природе

(3) любой общественной организации

(4) для государственных органов и муниципальных образований

66. С точки зрения информационного права информация – это:

(1) сведения о законодательстве, правовых явлениях, правоприменительной деятельности

(2) данные о развитии конкретной правовой науки и ее практическом применении

(3) сведения независимо от формы их представления

(4) форма выражения объективных знаний

67. Не являются объектами информационного правоотношения:

(1) неправовая информация

(2) обладатели информации

(3) информационные системы

(4) элементы информационной системы

(5) информационные продукты

(6) недокументированная информация

68. Признак, не относящийся к коммерческой тайне:

(1) информация имеет действительную или потенциальную коммерческую ценность

(2) сведения, содержащие коммерческую тайну, устанавливаются учредительными документами

(3) отсутствует свободный доступ к информации

(4) обладатель информации принимает меры к охране ее конфиденциальности

69. К служебной тайне не относится:

(1) профессиональная тайна

(2) тайна деятельности соответствующего органа

(3) вред, причиненный здоровью работника в связи с производственной травмой

70. В правовой режим документированной информации входит:

(1) государственная тайна

(2) тайна частной жизни

(3) банковская тайна

(4) электронная цифровая подпись

(5) персональные данные

71. Исключите неправильный постулат:

(1) информация не связана с определенным конкретным носителем

(2) информация не существует без материального носителя

(3) содержание информации меняется одновременно со сменой материального носителя

72. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:

(1) которые составляют финансово-экономическую информацию и позволяют избежать неоправданных расходов

(2) безопасности пищевых продуктов

(3) о показателях производственного травматизма, профессиональной заболеваемости

(4) о системе оплаты и условиях труда

73. Лица, занимающиеся предпринимательской деятельностью, могут устанавливать режим коммерческой тайны в отношении сведений:

(1) о размере и составе имущества некоммерческих организаций

(2) об оплате труда работников некоммерческих организаций

(3) об использовании безвозмездного труда граждан в деятельности некоммерческой организации

(4) об использовании новых технологий, позволяющих получить коммерческую выгоду

74. Формы защиты интеллектуальной собственности:

(1) авторское, патентное право и коммерческая тайна

(2) интеллектуальное право и смежные права

(3) коммерческая и государственная тайна

(4) гражданское и административное право

75. По доступности информация классифицируется на:

(1) открытую информацию и государственную тайну

(2) конфиденциальную информацию и информацию свободного доступа

(3) информацию с ограниченным доступом и общедоступную информацию

(4) виды информации, указанные в остальных пунктах

76. К конфиденциальной информации относятся документы, содержащие:

(1) государственную тайну

(2) законодательные акты

(3) «ноу-хау»

(4) сведения о золотом запасе страны

77. Запрещено относить к информации ограниченного доступа:

(1) информацию о чрезвычайных ситуациях

(2) информацию о деятельности органов государственной власти

(3) документы открытых архивов и библиотек

(4) все, перечисленное в остальных пунктах

78. К конфиденциальной информации не относится:

(1) коммерческая тайна

(2) персональные данные о гражданах

(3) государственная тайна

(4) «ноу-хау»

79. Согласно ст.132 Гражданского Кодекса РФ интеллектуальная собственность это:

(1) информация, полученная в результате интеллектуальной деятельности индивида

(2) литературные, художественные и научные произведения

(3) изобретения, открытия, промышленные образцы и товарные знаки

(4) исключительное право гражданина или юридического лица на результаты интеллектуальной деятельности

80. Интеллектуальная собственность включает права, относящиеся к:

(1) литературным, художественным и научным произведениям, изобретениям и открытиям

(2) исполнительской деятельности артиста, звукозаписи, радио- и телепередачам

(3) промышленным образцам, товарным знакам, знакам обслуживания, фирменным наименованиям и коммерческим обозначениям

(4) всему, указанному в остальных пунктах

81. Конфиденциальная информация это:

(1) сведения, составляющие государственную тайну

(2) сведения о состоянии здоровья высших должностных лиц

(3) документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ

(4) данные о состоянии преступности в стране

82. Какая информация подлежит защите:

(1) информация, циркулирующая в системах и сетях связи

(2) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

(3) только информация, составляющая государственные информационные ресурсы

(4) любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу

83. Формой правовой защиты литературных, художественных и научных произведений является право:

(1) литературное

(2) художественное

(3) авторское

(4) патентное

84. Запрещено относить к информации с ограниченным доступом:

(1) законодательные акты, информацию о чрезвычайных ситуациях и информацию о деятельности органов государственной власти (кроме государственной тайны)

(2) только информацию о чрезвычайных ситуациях

(3) только информацию о деятельности органов государственной власти (кроме государственной тайны)

(4) документы всех библиотек и архивов

85. Формой правовой защиты изобретений является:

(1) институт коммерческой тайны

(2) патентное право

(3) авторское право

(4) все, перечисленное в остальных пунктах

86. К коммерческой тайне могут быть отнесены:

(1) сведения, не являющиеся государственными секретами

(2) сведения, связанные с производством и технологической информацией

(3) сведения, связанные с управлением и финансами

(4) сведения, перечисленные в остальных пунктах

87. Является ли авторское право, патентное право и КТ формами защиты интеллектуальной собственности:

(1) да

(2) нет

(3) только авторское и патентное

(4) только КТ

88. Каким законом в РФ защищаются права исполнителей и производителей фонограмм:

(1) «О правовой охране программ для ЭВМ и баз данных»

(2) «Об авторском праве и смежных правах»

(3) «Патентный закон РФ»

(4) закон еще не принят

89. Контроль за защитой информации осуществляется:

(1) органами государственной власти

(2) международным сообществом

(3) органами местного самоуправления

90. Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, имеют право:

(1) принимать на работу лиц, ответственных за сохранность информации

(2) создавать специальные службы, обеспечивающие ее защиту

(3) создавать отделения охраны

91. Несоблюдение правил работы с информацией, повлекшее нарушение прав лиц, к которым эта информация относится, предусматривает:

(1) материальную ответственность

(2) дисциплинарную ответственность

(3) уголовную ответственность

92. Вторая степень защиты сведений, составляющих государственную тайну, имеет гриф:

(1) совершенно секретно

(2) особой важности

(3) для служебного пользования

93. Персональные данные работника являются:

(1) открытой информацией

(2) секретной информацией

(3) информацией с ограниченным доступом

94. Материальные объекты, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов – это:

(1) средства защиты грифы секретности

(2) системы защиты государственной тайны

(3) носители сведений, составляющих государственную тайну

95. Судебная защита прав субъектов в сфере информационных процессов и информатизации не осуществляется:

(1) судом общей юрисдикции

(2) Арбитражным судом

(3) Конституционным судом РФ

96. Информация о деятельности органов государственной власти и органов местного самоуправления является:

(1) открытой

(2) особо секретной

(3) конфиденциальной

97. Режим защиты информации НЕ устанавливается в отношении:

(1) конфиденциальной документированной информации

(2) персональных данных

(3) недокументированной информации

98. Коллегиальным органом, координирующим деятельность органов государственной власти по защите государственной тайны, является:

(1) Конституционный суд РФ

(2) Межведомственная комиссия

(3) Верховный суд РФ

99. К способам неправомерного доступа к информации относится:

(1) представление фиктивных документов на право доступа к информации

(2) пользование информацией с разрешения собственника

(3) разрешение владельца на доступ к информации

100. К государственной тайне и засекречиванию относятся сведения:

(1) о фактах нарушения прав и свобод человека и гражданина

(2) о защите Государственной границы РФ, исключительной экономической зоны и континентального шельфа РФ

(3) о размерах золотого запаса и государственных валютных резервах РФ

Задания в открытой форме

1) …… – это деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.
2) …… – обеспечение безопасности персонала, материальных и финансовых ресурсов от возможных угроз всеми доступными законными средствами, методами и мероприятиями, а также обеспечение безопасности информационных ресурсов в течение всего их жизненного цикла, на всех технологических этапах их обработки и использования, во всех режимах функционирования.
3) …… – комплекс мероприятий, ориентированных на пресечение разглашения, защиту информации от утечки и противодействия несанкционированному доступу.

4) …… – средства, в которых основная защитная функция реализуется некоторым техническим устройством (комплексом, системой).
5) …… – такой вид криптографического закрытия, при котором преобразованию подвергается каждый символ защищаемого сообщения.
6) …… – проверяют, имеется ли в файлах на указанном пользователем диске специфическая для данного вируса комбинация байтов.
7) …… – коммерческой тайной понимается информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.
8) …… – информацией понимаются сведения, находящиеся в собственности, использовании или в распоряжении отдельных физических или юридических лиц и распространяются по их желанию в соответствии с предусмотренными ими условиями.
9) …… – комплекс мероприятий, исключающих оглашение охраняемых сведений их владельцами.
10) …… – умышленные или неосторожные действия должностных лиц и граждан, результатом которых явилось неправомерное оглашение конфиденциальных сведений, и как следствие – ознакомление с ними лиц, не допущенных к этим сведениям.
11) …… – самостоятельное структурное подразделение, которое решает задачи по непосредственному обеспечению защиты жизненно важных интересов предприятия в условиях коммерческого и производственного риска, конкурентной борьбы.
12) …… – меры ограничительного характера, сводящиеся к регламентации доступа и использования технических средств обеспечения производственной деятельности и обработки конфиденциальной информации в традиционных или автоматизированных режимах.
13) …… – мероприятия обеспечивают блокирование возможных каналов утечки информации через технические средства обеспечения производственной и трудовой деятельности с помощью специальных технических средств, устанавливаемых на элементы конструкции зданий, помещений и технических средств, потенциально образующих возможные каналы утечки информации.
14) …… – мероприятия обеспечивают приобретение, установку и использование в процессе производственной деятельности специальных, защищенных от побочных излучений и наводок, технических средств обработки конфиденциальной информации или средств ПЭМИН которых не превышают норм на границе охраняемой территории.
15) …… – помещения (служебные кабинеты, конференц-залы и т.п.), специально предназначенные для работы с документами ограниченного доступа, для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров).

16) …… – система, обеспечивающая санкционированный вход в здание и в зоны ограниченного доступа и выход из них путем идентификации личности по комбинации различных признаков: вещественный код (виганд-карточки, touch-memory и т.п.), запоминаемый код (клавиатуры, кодонаборные панели), биометрические признаки (отпечатки пальцев и т.п.) и предотвращающая несанкционированный проход в помещения и зоны объекта.

17) …… – лицо, которому необходимо решить определенный круг деловых или личных вопросов с руководителями и менеджерами фирмы, а также лицо, совместно с которым полномочные лица вырабатывают определенные решения по направлениям деятельности фирмы.

18) …… – различные действия, которые могут привести к нарушениям информационной безопасности.

19) …… – проверки осуществляются при смене руководителей подразделений или направлений деятельности фирмы, увольнении сотрудников, после завершения экстремальной ситуации, при выявлении фактов возможной утраты информации и в других случаях.

20) …… – совокупность используемых для охраны предприятия сил и средств, а также способов и методов охраны предприятия и его объектов. Она включает: личный состав подразделений охраны, технические средства охраны, места размещения личного состава, выполняющего задачи охраны, и используемых технических средств, методы охраны объектов.

21) …… – несанкционированный выход защищаемых сведений и документов за пределы круга лиц, которым они доверены или стали известны в ходе их трудовой деятельности.

Задание на установление соответствия

1) Установите соответствие

1) Информация признается охраняемой законом при условии, что она	a) уголовная
2) Для защиты сведений, составляющих государственную тайну, не предусмотрен гриф	b) Для служебного пользования
3) За разработку и распространение компьютерных вирусов предусмотрена ответственность	c) изъята из публичного оборота

2) Установите соответствие

1) Решение о передаче сведений, составляющих государственную	a) уголовная ответственность

тайну, другому государству принимает	
2) Под неправомерным доступом к информации в законодательстве понимают	b) самовольное получение информации без разрешения ее собственника или владельца
3) За разглашение сведений, составляющих государственную тайну, предусмотрена	c) Правительство РФ

3) Установите соответствие

1) Владельцем информационных ресурсов, информационных систем и технологий является	a) документы в информационных системах и банках данных
2) В соответствии с Федеральным законом РФ «О государственной тайне» к числу основных принципов отнесения информации к государственной тайне относятся	b) Законность, обоснованность и своевременность
3) Предметом преступлений в сфере компьютерной информации являются	c) осуществляющий владение, пользование и распоряжение ими

4) Установите соответствие

1) Коммерческую тайну организации или предпринимателя могут составлять	a) в военной области
2) Преступления в сфере компьютерной информации относятся к преступлениям	b) против общественной безопасности
3) Государственную тайну составляют сведения	c) данные о клиентской базе предприятия

5) Установите соответствие

1) Защита компьютерной информации введена	a) не сообщать персональные данные работника без его письменного согласия
2) Установление ограничений на распространение сведений с момента их получения (разработки) или заблаговременно	b) принцип своевременности отнесения сведений к государственной тайне
3) Работодатель при передаче	c) Уголовным кодексом Российской

персональных данных работника обязан	Федерации

6) Установите соответствие

1) Отказ в доступе к открытой информации может быть обжалован в	a) восстановления нарушенных прав и возмещения причиненного ущерба
2) Порядок хранения и использования персональных данных работников устанавливается	b) работодателем с соблюдением требований Трудового кодекса Российской Федерации
3) Защита прав в сфере пользования информационными ресурсами осуществляется в целях	c) суде

7) Установите соответствие

1) Почему на пакетах (конвертах) с конфиденциальными документами не проставляют гриф конфиденциальности?	a) на Перечень и на решение руководителя
2) Что делать с ошибочно присланными конфиденциальными документами?	b) Их нужно отправить обратно или переслать в нужный адрес по согласованию с отправителем
3) На что будут ссылаться при регистрации входящих документов, потенциально содержащих конфиденциальную информацию?	c) чтобы не привлекать внимания

8) Установите соответствие

1) Что происходит с конфиденциальными документами, которые не исполнены в текущем делопроизводственном году?	a) нет, не стоит, нужно составить акты и вернуть обратно
2) Что подразумевает экспедиционная обработка?	b) учет и регистрацию входящих/исходящих пакетов и документов
3) Стоит ли принимать надорванный пакет (конверт) с конфиденциальными документами, если он адресован в вашу организацию?	c) их переводят для исполнения в новом делопроизводственном году

9) Установите соответствие

1) Какая отметка должна стоять в журнале учета входящих документов, если конфиденциальный документ пришел с сопроводительным письмом, которое, в свою очередь, не содержит конфиденциальной информации?	a) нет
2) За что отвечает служба конфиденциального делопроизводства?	b) за учет и регистрацию конфиденциальных документов, за передачу документов между исполнителями, за контроль за сроками исполнения документов
3) Обязательно ли вести два отдельных журнала для учета пакетов конфиденциальных документов и самих документов?	c) «без приложения не конфиденциально»

10) Установите соответствие

1) Термин «информация» определен как «сведения (сообщения, данные) независимо от формы их представления»	a) непрерывность, комплексность, системность, законность
2) Каким нормативным актом регулируются отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации?	b) Конституцией РФ, ФЗ РФ «О безопасности» и «О государственной тайне»
3) Система обеспечения информационной безопасности информации должна базироваться на следующих принципах:	c) Федеральным законом РФ N 149-ФЗ «Об информации, информационных технологиях и защите информации»

11) Установите соответствие

1) Каким нормативным актом регулируются отношения, связанные с отнесением информации к коммерческой тайне, передачей	a) совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и

такой информации, охраной ее конфиденциальности в целях обеспечения баланса интересов обладателей информации, составляющей коммерческую тайну, и других участников регулируемых отношений, в том числе государства, на рынке товаров, работ, услуг и предупреждения недобросовестной конкуренции, а также определяет сведения, которые не могут составлять коммерческую тайну?	технических средств
2) Какие степени секретности сведений, составляющих государственную тайну, существуют?	b) особой важности, совершенно секретно, секретно
3) Что такое информационная система персональных данных?	c) Конституцией РФ, Гражданским кодексом, ФЗ РФ «О коммерческой тайне»

12) Установите соответствие

1) Что такое государственная тайна?	a) защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей, не связанных с государственной или муниципальной службой, распространение которой может нанести ущерб правам и законным интересам другого лица (доверителя), доверившего эти сведения, и не являющаяся государственной или коммерческой тайной
2) Основными составляющими информационной безопасности являются:	b) конфиденциальность, целостность, доступность
3) Профессиональной тайной может быть:	c) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и

	оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности РФ

13) Установите соответствие

1) Что такое ИСПДн?	a) все меры, направленные на обеспечение информационной безопасности, должны планироваться с ранних стадий системы безопасности и вводиться своевременно
2) Что такое целостность информации?	b) свойство информационных ресурсов, заключающееся в их неизменности в процессе передачи или хранения
3) Принцип системы обеспечения информационной безопасности «своевременности» предполагает, что:	c) информационная система персональных данных

14) Установите соответствие

1) Что такое коммерческая тайна?	a) специальные, типовые
2) Что такое доступность информации?	b) свойство информационных ресурсов, заключающееся в их получении и использовании по требованию уполномоченных лиц
3) Какие типы ИС существуют?	c) конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

15) Установите соответствие

1) Какой из нормативно-правовых документов определяет перечень объектов информационной	a) тайна страхования, тайна исповеди, врачебная тайна, тайна связи, адвокатская тайна

безопасности и методы ее обеспечения?	
2) К объектам служебной тайны относятся:	b) тайна следствия, военная тайна, судебная тайна
3) К объектам профессиональной тайне относятся:	c) Доктрина информационной безопасности РФ

16) Установите соответствие

1) Что такое конфиденциальность информации?	a) электронный документ, содержащий открытый ключ ЭЦП пользователя
2) Какой класс присваивается информационным системам, если нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных?	b) К2
3) Сертификат ЭЦП – это:	c) свойство информационных ресурсов, заключающееся в их недоступности для неуполномоченных лиц

17) Установите соответствие

1) Какой класс присваивается информационным системам, если нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных?	a) физическое лицо
2) К какой категории относятся персональные данные, позволяющие идентифицировать субъекта персональных данных?	b) 3 категория
3) Кто является субъектом персональных данных?	c) К1

18) Установите соответствие

1) Какие классы ИСПДн вы знаете?	a) 4 категория
2) На какие группы подразделяются информационные ресурсы государства?	b) открытая информация, запатентованная информация, информация защищаемая
3) К какой категории относятся обезличенные (общедоступные) персональные данные?	c) 1-4 классы

19) Установите соответствие

1) Какие органы осуществляют контроль и надзор за соблюдением требований ФЗ-152?	a) К3
2) Какие процедуры включает в себя система ЭЦП?	b) процедуру формирования и проверки цифровой подписи
3) Какой класс присваивается информационным системам, если нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных?	c) ФСБ, ФСТЭК, Роскомнадзор

20) Установите соответствие

1) Кто является оператором персональных данных?	a) мероприятия, связанные с выдачей лицензий на осуществление лицензируемых видов деятельности и надзор за соблюдением лицензиатами соответствующих лицензионных требований и условий
2) Для чего используется сертификат открытого ключа ЭЦП?	b) для аутентификации
3) Что такое лицензирование?	c) государственный или муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели и содержание обработки персональных данных

21) Установите соответствие

1) Какие схемы (модели) УЦ существуют в настоящее время?	a) 2 категория
2) К какой категории относятся персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни?	b) 1 категория
3) К какой категории относятся персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию?	c) иерархическая, сетевая, гибридная, мостовая

Задания на установление правильной последовательности

1. Установить последовательность решения задач по обеспечению безопасности информации на организационном уровне:

1. сертификация средств защиты информации;
2. контроль выполнения установленных правил работы в компьютерных системах.
3. оценка эффективности функционирования системы защиты информации;
4. совершенствование системы защиты информации;
5. разработка документации;
6. организация работ по разработке системы защиты информации;
7. ограничение доступа на объект и к ресурсам информации;
8. лицензирование деятельности по защите информации;3. разграничение доступа к ресурсам информации;
9. аттестация объектов защиты;
10. планирование мероприятий;
11. воспитание и обучение обслуживающего персонала и пользователей;

2. Установить последовательность принципов организации и функционирования системы безопасности

1. активность
2. своевременность
3. взаимодействие и координация
4. специализация
5. комплексность
6. обоснованность

7. законность
8. непрерывность
9. экономическая целесообразность

3. Установить последовательность блоков структуры правовых актов, ориентированных на правовую защиту:
1. законодательство субъектов РФ, касающееся защиты информации
2. правоохранительное законодательство, содержащее нормы об ответственности за правонарушения в сфере информатизации
3. специальные законы, полностью относящиеся к конкретным сферам отношений
4. подзаконные нормативные акты по защите информации
5. законы об организации управления, касающиеся отдельных структур
6. конституционное законодательство
7. общие законы, кодексы

4. Установить последовательность переченя сведений составляющих государственную тайну:
1. сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности
2. сведения в области внешней политики и экономики
3. сведения в военной области
4. сведения в области экономики, науки и техники

5. Установить последовательность учета физической природы образования канала утечки информации:
1. материально-вещественные
2. электромагнитные
3. радиоканалы
4. акустические
5. оптические

6. Установить последовательность шпионажа способами несанкционированного доступа:
1. подделка
2. хищение
3. фотографирование (видеонаблюдение)
4. сбор и аналитическая обработка
5. копирование
6. наблюдение
7. инициативное сотрудничество
8. перехват
9. склонение к сотрудничеству
10. уничтожение
11. выведывание, выпытывание

12. негласное ознакомление
13. подслушивание
14. незаконное подключение

7. Установить последовательность показателей системной классификации технических средств защиты:
1. тип средства защиты, указывающий на принципы работы элементов
2. стоимость приобретения, установки и эксплуатации
3. функциональное назначение
4. сложность средства защиты и практического его использования
5. сопряженность средств защиты с другими средствами объекта обработки информации

8. Установить последовательность аппаратных средств защиты:
1. маскировка сигнала, содержащего конфиденциальную информацию
2. нейтрализация технических каналов утечки информации
3. поиск закладных устройств

9. Установить последовательность физических средств защиты:
1. опознавание
2. внутренняя защита
3. внешняя защита

10. Установить последовательность детективной и охранной деятельности:
1. установление обстоятельств разглашения коммерческих секретов
2. выявление недобросовестных и неплатежеспособных партнеров
3. изучение рынка
4. установление обстоятельств недобросовестной конкуренции
5. сбор сведений по гражданским делам
6. сбор сведений о партнерах и конкурентах

11. Установить последовательность этапов при профотборе сотрудников для работы на коммерческих предприятиях:
1. сбор и оценка информации о кандидатах
2. исследование результатов тестирований
3. тестовые примеры и иные научные методики проверки кандидатов
4. предварительное собеседование
5. заключительное собеседование

12. Установить последовательность построения службы безопасности:
1. разработать структуру службы безопасности, исходя из полученных данных, финансовых и трудовых возможностей
2. поддерживать работоспособность службы безопасности корректировать ее структуру в зависимости от изменяющихся условий
3. провести анализ угроз и выявить степень риска при их реализации

4. определить жизненно важные интересы предприятия на момент создания службы безопасности
5. наметить пути локализации каждой из угроз и просчитать затраты на проведение соответствующих мероприятий
6. выявить угрозы безопасности для данного объекта

13. Установить последовательность структурных единиц организационной службы безопасности:
1. группа безопасности внешней деятельности
2. отдел режима и охраны, в составе сектора режима и сектора охраны
3. инженерно-техническая группа
4. отдел защиты информации

14. Установить последовательность мероприятий по изучению окружения объекта, проводимые сотрудниками группы безопасности:
1. определяют платежеспособность юридических и физических лиц, их возможности по своевременному выполнению платежных обязательств
2. проводят ситуационный анализ текущего состояния финансово-торговой деятельности с точки зрения прогнозирования возможных последствий, могущих привести к неправомерным действиям со стороны конкурирующих организаций и предприятий
3. ведут учет и анализ попыток несанкционированного получения коммерческих секретов конкурентами
4. изучают торгово-конъюнктурные ситуации в пространстве деятельности учредителей, партнеров, клиентов и потенциально возможных конкурентов
5. определяют возможные направления и характер злоумышленных действий со стороны специальных служб промышленного шпионажа против предприятия, его партнеров и клиентов
6. собирают и обрабатывают сведения о деятельности потенциальных и реальных конкурентов для выявления возможных злонамеренных действий по добыванию охраняемых сведений

15. Установить последовательность организационной структуры, численности и состава службы безопасности:
1. начальник службы безопасности
2. служба безопасности предприятия в составе подразделений
3. линейные подразделения предприятия, активно участвующие в обеспечении экономической безопасности
4. руководитель предприятия
5. антикризисная группа

16. Установить последовательность решаемых задач антикризисной группой:
1. обеспечение оперативного взаимодействия с органами правопорядка

2. принятие неотложных мер по безопасности
3. оценку обстановки
4. управление деятельностью предприятия в экстренных условиях

17. Установить последовательность принципов организации защиты информации, обрабатываемой в информационных системах:

1. защита информационных систем должна предусматривать контроль эффективности средств защиты от несанкционированного доступа
2. программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики информационных систем
3. защита средств вычислительной техники, входящей в состав информационных систем, обеспечивается комплексом программно-технических средств
4. защита информационных систем основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от несанкционированного доступа к информации
5. защита информационных систем обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер
6. неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты
7. защита ис должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ

18. Установить последовательность аналитической работы направлений обнаружения канала или каналов несанкционированного доступа к ценной информации фирмы:

1. анализ каналов объективного распространения информации
2.анализ источников конфиденциальной информации
3. аналитическая работа с источником угрозы информации

19. Установить последовательность аналитической работы с источником угрозы конфиденциальной информации:

1. учет и изучение каждого отдельного субъективного внутреннего и внешнего источника, степени его опасности (анализ риска) при реализации угрозы
2. выявление и классификацию максимального состава источников угрозы конфиденциальной информации

3. разработку превентивных мероприятий по локализации и ликвидации объективных угроз

20. Установить последовательность правил, выполняемых сотрудниками, занятых в работе с документами, содержащими конфиденциальную информацию:

1. сотрудник организации обязан вести и хранить все записи, журналы и файлы, содержащие служебную информацию, в полном соответствии с требованиями действующего законодательства, внутренних документов организации и указаниями руководства
2. объем информации, предоставляемый клиентам организации или предприятия, определяется характером предоставляемых услуг и указаниями руководителей соответствующих подразделений
3. служебная информация, доступная одному подразделению, ни при каких обстоятельствах не может другое, за исключением случаев, когда это диктуется технологией совершения операций в организации, либо при наличии необходимости с санкции руководителя данного подразделения
4. служебная информация, которая известна сотруднику по роду работы, является конфиденциальной и не подлежит разглашению, в том числе и другим сотрудникам, нужна для исполнения ими своих служебных обязанностей

21. Установить последовательность основных форм контроля качества работы персонала, повышения их профессиональных знаний в части защиты информации:

1. регулярные проверки руководителем или службой безопасности соблюдения сотрудниками информации
2. самоконтроль сотрудников
3.аттестация сотрудников
4. отчеты руководителей подразделений о работе подразделений и состоянии системы защиты информации

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

Максимальный балл за тестирование представляет собой разность двух чисел: максимального балла по промежуточной аттестации для данной

формы обучения (36) и максимального балла за решение компетентностно-ориентированной задачи (6).

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

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

Соответствие 100-балльной и 5-балльной шкал

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

2.2 КОМПЕТЕНТНОСТНО-ОРИЕНТИРОВАННЫЕ ЗАДАЧИ

Компетентностно-ориентированная задача № 1

В некоторой фирме происходит утечка информации, самые выгодные контракты срываются, их заключают конкуренты. Руководитель фирмы обратился в детективное агентство с целью установления личности тех, кто передает ценные сведения конкурентам. Частный детектив организовал прослушивание офисных помещений и квартир сотрудников фирмы. В ходе круглосуточного наблюдения был установлен круг подозреваемых, в квартире которых позже детектив произвел обыск. Он обнаружил документы, подтверждающие причастность лица к передаче конфиденциальной информации. Среди личных документов были обнаружены фотографии, которые указывали на весьма свободный образ жизни человека. Детектив переснял эти фотографии и с разрешения начальника фирмы разместил в Интернете. Сотрудник фирмы, уличенный в преступлении, был уволен. Найти и определить тип информационных преступлений. Предложить меры по предотвращению подобных преступлений.

Компетентностно-ориентированная задача № 2

Известный политический деятель Х баллотируется на пост президента государства. Один из его конкурентов организовал «охоту журналистов». На всех приемах и закрытых вечеринках его фотографировали, пытаясь поймать момент, который бы его дискредитировал в глазах избирателей. Параллельно шел сбор информации о личной жизни кандидата и его семьи. Любая информация сразу же появлялась в средствах массовой информации. Одному из журналистов удалось узнать, что дети кандидата неродные, а

усыновленные, об этом сообщили на страницах всех электронных изданий. Последним шагом в предвыборной борьбе стало распространение листовок, в которых кандидат яко бы призывал к насильственному захвату власти. Как выяснилось позже, подобные листовки не имели никакого отношения к избирательной политике господина Х. Размещенные в Интернете фотографии были подделаны с помощью компьютерной программы. Господин Х в результате организованной конкурентами войны снял свою кандидатуру и ушел из политики. Найти и определить тип информационных преступлений. Предложить меры по предотвращению подобных преступлений.

Компетентностно-ориентированная задача № 3

Российский физик-ядерщик У был задержан западными спецслужбами. Ему предъявили обвинение в подделке банковских бумаг. По заявлению представителей спецслужб на квартире ученого была обнаружена оргтехника, с помощью которой он производил подделку документов. Вскоре СМИ перестали освещать этот скандал, а физика-ядерщика выдворили из страны. Вернувшись на родину, господин У продолжил работу в лаборатории. Через некоторое время был установлен факт утечки секретной информации об изготовлении оружия массового поражения. За господином У была установлена слежка и организовано прослушивание всех телефонных разговоров. В ходе проводимой операции были изъяты личные документы ученого, в том числе и незапатентованные им изобретения. На некоторые изобретения господина У были заявлены авторские права других работников лаборатории. Сам физик был арестован. Ему было предъявлено обвинение в шпионаже. Найти и определить тип информационных преступлений. Предложить меры по предотвращению подобных преступлений.

Компетентностно-ориентированная задача № 4

В одной из фирм, занимающихся разработкой прикладных программ, группа программистов, используя свое служебное положение, подобрала код к банковским счетам некоторых клиентов. В течение некоторого времени они переводили деньги на счета подставных лиц. Чтобы скрыть следы своего преступления, программисты запустили вирус, который разрушил базу данных банка. Кроме того, им удалось прослушать переговоры между банковскими служащими. По решению правления банка, историю с взломом счетов и распространением вируса, решили замолчать, чтобы не портить репутацию банка. Программисты стали шантажировать председателя правления, требуя дополнительных денежных переводов. В противном случае, они обещали распространить подробную информацию в глобальной сети. В ходе проводившейся налоговой проверки были установлены факты правонарушений со стороны руководства банка, за что оно было привлечено к ответственности. Вину программистов доказали частично. Найти и определить тип информационных преступлений. Предложить меры по предотвращению подобных преступлений.

Компетентностно-ориентированная задача № 5
Костюничев, работающий в одном из государственных унитарных предприятий, куда отчислялись средства из государственного бюджета, открыл новые технические возможности одного из производственных станков, данное открытие позволило значительно увеличить производительность ГУПа в целом. Директор предприятия решил скрыть от руководства данное нововведение и юридически оформил режим коммерческой тайны, тем самым, скрыв часть дополнительной прибыли. Через месяц органы прокуратуры, заподозрив проявление коррупциогенного фактора, направили мотивированное требование о предоставлении информации государственным предприятием. В скором времени прокуратура обратилась с заявлением в суд об истребовании информации, составляющую коммерческую тайну. Какое решение вынесет суд в отношении данного вида информации? Подлежит ли директор ответственности по ч.2 статье 285 УК РФ?

Компетентностно-ориентированная задача № 6
Смирнова Анна работала в ООО «Марашка» оператором call-центра. Ежедневно она принимала звонки сотни клиентов, которые делали заказы в интернет - магазине товаров для животных «Марашка». Каждый заказ записывался в таблицы excel для ведения учета. Гриф о том, что данная информация составляет коммерческую тайну, нанесен не был. 13.04.2015 Смирнова решила отправить своей подруге эту таблицу «ради интереса». Начальник Смирновой Печенюшкин узнал об этом и уволил ее по подпункту «в» части 6 статьи 81 Трудового кодекса (за разглашение коммерческой тайны). Анна обратилась в суд с иском о восстановлении ее на рабочем месте. Какое решение вынесет суд и почему?

Компетентностно-ориентированная задача № 7
Командир войсковой части С., имея допуск к сведениям, составляющим государственную тайну, привлек подчиненных военнослужащих рядовых Са. и Ш. к изготовлению на категорированной ПЭВМ личного плана работы командира командного пункта на период его перевода с мирного на военное время. В результате этого указанные военнослужащие узнали сведения, подпадающие под п. 5 "Перечня сведений, отнесенных к государственной тайне", утвержденного Указом Президента РФ от 30 ноября 1995 года N 1203 "Об утверждении перечня сведений, отнесенных к государственной тайне". Приговором окружного военного суда полковник С. был признан виновным в разглашении сведений составляющих государственную тайну.

Компетентностно-ориентированная задача № 8
На предприятии ООО «Константа» установлен режим коммерческой тайны относительно сведений, касающихся бухгалтерской отчетности предприятия. Для введения режима коммерческой тайны были установлены следующие

сведения: перечень лиц, получивших доступ к коммерческой тайне, порядок обращения с данной информацией и контроль за соблюдением порядка доступа к секретной информации. Кроме того, с допущенными лицами заключены соответствующие трудовые договоры. На каждом листе установлен гриф секретности. Соловьев, сотрудник компании ООО «Константа», допущенный к сведениям, составляющим коммерческую тайну, распространил секретную информацию конкурентам. В связи с этим он был уволен с работы по подпункту «в» п.6 ч.1 ст. 81 ТК РФ. Соловьев оспорил данное решение в суде и был восстановлен. Правильное ли решение принял суд? Ответ обоснуйте.

Компетентностно-ориентированная задача № 9

В организации ООО «Альфа» был введен режим коммерческой тайны относительно сведений бухгалтерской отчетности юридического лица, т.е. были определены порядок обращения с этой информацией и контроля за соблюдением такого порядка; перечень лиц, получивших доступ к коммерческой тайне; заключены с ними соответствующие трудовые договоры; а так же на каждом из таких документов присутствовал гриф «коммерческая тайна». Один из сотрудников ООО «Альфа» Петров, имеющий доступ к коммерческой тайне, был уличен в распространении данной информации конкурентам. В связи с этим он был уволен по подпункту «в» п. 6 ч. 1 ст. 81 ТК РФ. Петров оспорил данное решение в суде и выиграл дело. Обоснуйте, правильное ли решение принял суд?

Компетентностно-ориентированная задача № 10

Администрация г. Воронеж запросила документы о деятельности компании «Элита». Компания отказалась предоставить документы, ссылаясь на то, что в документах содержатся сведения, составляющие коммерческую тайну. Правомерен ли отказ компании?

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

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

Балл, полученный обучающимся за решение компетентностно-ориентированной задачи, суммируется с баллом, выставленным ему по результатам тестирования. Общий балл промежуточной аттестации суммируется с баллами, полученными обучающимся по результатам

текущего контроля успеваемости в течение семестра; сумма баллов переводится в оценку по 5-балльной шкале следующим образом:

Соответствие 100-балльной и 5-балльной шкал

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

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

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

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

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

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