ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ МОСКОВСКОЙ ОБЛАСТИ
«ДМИТРОВСКИЙ ТЕХНИКУМ»

Александровская И.Л.
2021.04.20 09:10:
39+03'00'

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ПРОФЕССИОНАЛЬНОМУ МОДУЛЮ

ПМ. 01 Участие в планировании и организации работ по обеспечению защиты объекта

специальность 10.02.01 Организация и технология защиты информации

Дмитров, 2020г.

Комплект контрольно-оценочных средств разработан на основе Федерального государственного образовательного стандарта среднего профессионального образования по специальности **10.02.01 Организация и технология защиты информации** *(Уровень подготовки - базовый)* программы учебной дисциплины **Участие в планировании и организации работ по обеспечению защиты объекта**

СОДЕРЖАНИЕ

1. ПАСПОРТ

Комплект оценочных средств представляет собой совокупность контрольно-оценочных средств для определения качества освоения студентом профессионального модуля по специальности 10.02.01 «Организация и технология защиты информации».

В результате освоения профессионального модуля обучающийся должен обладать предусмотренными ФГОС по специальности следующими умениями и знаниями**:**

уметь:

- организовывать охрану персонала, территорий, зданий, помещений и продукции организаций;
- пользоваться аппаратурой систем контроля доступа;
- выделять зоны доступа по типу и степени конфиденциальности работ;
- определять порядок организации и проведения рабочих совещаний;
- использовать методы защиты информации в рекламной и выставочной деятельности;
- использовать критерии подбора и расстановки сотрудников подразделений защиты информации;
- организовывать работу с персоналом, имеющим доступ к конфиденциальной информации;
- проводить инструктаж персонала по организации работы с конфиденциальной информацией;
- контролировать соблюдение персоналом требований режима защиты информации;

знать:

- виды и способы охраны объекта;
- особенности охраны персонала организации;
- основные направления и методы организации режима и охраны объекта;
- разрешительную систему доступа к конфиденциальной информации;
- принципы действия аппаратуры систем контроля доступа;
- принципы построения и функционирования биометрических систем безопасности;
- требования и особенности оборудования режимных помещений;
- требования и порядок реализации режимных мер в ходе подготовки и проведения совещаний по конфиденциальным вопросам и переговоров;
- требования режима защиты информации при приеме в организации посетителей;
- организацию работы при осуществлении международного сотрудничества;
- требования режима защиты информации в процессе рекламной деятельности;
- требования режима защиты конфиденциальной информации при опубликовании материалов в открытой печати;
- задачи, функции и структуру подразделений защиты информации;

- принципы, методы и технологию управления подразделений защиты информации;
- методы проверки персонала по защите информации;
- процедуру служебного расследования нарушения сотрудниками режима работы с конфиденциальной информацией.

иметь практический опыт:

- использования физических средств защиты объекта;
- применения физических средств контроля доступа на объект;
- ведения текущей работы исполнителей с конфиденциальной информацией;

Результатом освоения профессионального модуля является овладение обучающимися видом профессиональной деятельности (ВПД) **Участие в планировании и организации работ по обеспечению защиты объекта**, в том числе профессиональными (ПК) и общими (ОК) компетенциями:

Код	Наименование результата обучения
ПК 1.1.	Участвовать в сборе и обработке материалов для выработки решений по обеспечению защиты информации и эффективному использованию средств обнаружения возможных каналов утечки конфиденциальной информации
ПК 1.2.	Участвовать в разработке программ и методик организации защиты информации на объекте
ПК 1.3.	Осуществлять планирование и организацию выполнения мероприятий по защите информации
ПК 1.4.	Участвовать во внедрении разработанных организационных решений на объектах профессиональной деятельности
ПК 1.5.	Вести учет, обработку, хранение, передачу, использование различных носителей конфиденциальной информации
ПК 1.6.	Обеспечивать технику безопасности при проведении организационно-технических мероприятий
ПК 1.7.	Участвовать в организации и проведении проверок объектов информатизации, подлежащих защите
ПК 1.8.	Проводить контроль соблюдения персоналом требований режима защиты информации
ПК 1.9.	Участвовать в оценке качества защиты объекта
ОК 1.	Понимать сущность и социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности
ОК 2.	Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество
ОК 3.	Принимать решения в стандартных и нестандартных ситуациях и нести за них ответственность

ОК 4.	Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития
ОК 5.	Использовать информационно-коммуникационные технологии в профессиональной деятельности.
ОК 6.	Работать в коллективе и команде, эффективно общаться с коллегами, руководством, потребителями.
ОК 7.	Брать на себя ответственность за работу членов команды (подчиненных), результат выполнения заданий
ОК 8.	Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации
ОК 9.	Ориентироваться в условиях частой смены технологий в профессиональной деятельности.
ОК 10.	Применять математический аппарат для решения профессиональных задач
ОК 11.	Оценивать значимость документов, применяемых в профессиональной деятельности
ОК 12.	Ориентироваться в структуре федеральных органов исполнительной власти, обеспечивающих информационную безопасность

2. ЭКЗАМЕНАЦИОННЫЕ ЗАДАНИЯ

Инструкция

Часть А содержит 30 тестовых задании

Помещение: Компьютерный класс

Оборудование: компьютеры объединенные в локальную сеть

Программное обеспечение: программа контроля знаний Nettest

Норма времени:45 минут

Критерии оценки: за каждый правильный ответ на вопрос тестового задания ставиться 1 балл, за неверный 0 баллов максимальное количество баллов – 30

Часть Б содержит практическое задание которое выполняется индивидуально. Разработана в 23 вариантах

Помещение: Компьютерный класс

Оборудование: компьютеры, объединенные в локальную сеть с выходом в интернет.

Программное обеспечение: пакет Microsoftoffice, браузер Internetexplorer.

Норма времени 45 минут

Часть В содержит практическое задание которое выполняется индивидуально. Разработана в 12 вариантах.

Помещение: Компьютерный класс

Допускается использовании нормативно-правовых документо

Часть А Задания ознакомительного уровня (узнавание ранее изученных объектов, свойств)

1. Уязвимость информации - это:

А) Сведения об окружающем мире (объекте, процессе, явлении, событии) , которые являются объектом преобразования (включая хранение, передачу и т. д.) и используются для выработки поведения, для принятия решения, для управления или для обучения

Б) Это понятие, которое употребляется по отношению к отдельным лицам. Это есть право лица решать, какую информацию он желает разделить с другими, а какую хочет скрыть от других..

В) Объективное свойство информации подвергаться различного рода воздействиям, нарушающим ее целостность, достоверность и конфиденциальность.

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

А) Сотрудники

Б). Хакеры

В) Атакующие

Г) Контрагенты (лица, работающие по договору)

3. Сотрудники группы режима (функции):

А) наблюдение за обстановкой вокруг объекта и на его территории;

Б)определяют перечень сведений, составляющих коммерческую тайну, если таковые сведения не упомянуты в общегосударственных документах;

В) разрабатывают положения и инструкции о порядке работы с конфиденциальной информацией и сведениями, составляющими тайну;

Г) организуют и ведут закрытое делопроизводство, учет пользования, хранение и размножение документов и других, носителей конфиденциальной информации;

4. Сотрудники группы охраны и сопровождения участвуют в:

А) в организации прохода персонала и посетителей в различные зоны безопасности;

Б) в наблюдении за обстановкой вокруг объекта и на его территории;

В) в экстренных действиях при возникновении угроз чрезвычайных обстоятельств;

Г) осуществляют допуск персонала объекта к работе с конфиденциальной информацией, разрабатывают и осуществляют проверки выполнения сотрудниками объекта регламента работы с такой информацией;

5. К персональным данным относятся:

А) Ф.И.О..

Б) Адрес

В) Паспортные данные

Г)Семейное положение

Д)Сведения о доходах.

6. В минимальный штатный состав СБ входят:

А) *Директор*

Б) Аналитик

В) Оперативный дежурный

Г) Начальник отдела кадров

Д*) Юрист*

Е) Сотрудник делопроизводства

Ж) Сотрудник безопасности

7. Что из перечисленного не является целью проведения анализа рисков

А. Делегирование полномочий

Б. Количественная оценка воздействия потенциальных угроз

В. Выявление рисков

Г. Определение баланса между воздействием риска и стоимостью необходимых контрмер

8. Целями обеспечения безопасности предприятия является:

А)защита законных прав предприятия во взаимоотношениях с государственными органами, российскими и зарубежными партнерами и конкурентами; поддержание устойчивости порядка управления предприятием;

Б)сохранение собственности предприятия, ее рационального и эффективного использования в направлении удовлетворения общественных потребностей;

В) предотвращение утечки, хищения, утраты, искажения, подделки информации;

Г)повышение конкурентоспособности производимых товаров и услуг, создание благоприятной рыночной конъюнктуры для их реализации в условиях конкуренции на внутреннем и мировом рынке; рост прибылей предприятия;

Д)достижение внутренней и внешней организационной стабильности деятельности предприятия, надежности кооперированных связей и недопущение односторонней зависимости от случайных и недобросовестных партнеров;

Е) предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима документированной информации как объекта собственности;

9. Текущая работа с персоналом, обладающим конфиденциальной информацией, включает в себя:

А) Обучение и систематическое инструктирование сотрудников;

Б) Проведение регулярной воспитательной работы.

В)Постоянны контроль за выполнением персоналом требований по защите КИ.

Г) Проведение служебных расследований пофакта утечки информации

Д) Возможны все варианты.

10. Что самое главное должно продумать руководство при классификации данных?

А. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

В. Необходимый уровень доступности, целостности и конфиденциальности

С. Оценить уровень риска и отменить контрмеры
D. Управление доступом, которое должно защищать данные

11. **В качестве основных задач системыбезопасностирассматриваются:**

А) своевременное выявление и устранение угроз персоналу и ресурсам; причин и условий, способствующих нанесению финансового, материального и морального ущерба интересам предприятия, нарушению его нормального функционирования и развития;

Б) создание механизма и условий оперативного реагирования на угрозы безопасности и проявления негативных тенденций в функционировании предприятия;

В) пресечение посягательств на ресурсы и угроз персоналу на основе комплексного подхода к безопасности;

Г) создание условий для максимально возможного возмещения и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, для ослабления негативного влияния последствий нарушения безопасности на достижение стратегических целей.

12. Доступ к конфиденциальным базам данных и файлам является:

А) Этап изготовления и издания конфиденциальных документов характеризующим наличие комплекса специальных документов

Б) При использовании автоматизированной системы контроле в установленном графике.

В) Завершающим этапом доступа сотрудника фирмы к компьютеру

13. Сохранение коммерческой тайны, борьба с хакерами – это

А) Физическая безопасность

Б) *Информационная безопасность*

В) Экологическая безопасность

Г) Экономическая безопасность

14. Защищенность информации означает:

А) невозможность несанкционированного использования или изменения;

Б) независимость от чьего-либо мнения;

В) удобство формы или обмена;

Г) возможность получения данным потребителем.

15. В соответствии с Федеральным законом от 8.08.2001 года №128–ФЗ деятельность различных подразделений службы безопасности предприятия подпадает под требования:

А) Заключать договор о неразглашении государственной тайны

Б) Разрабатывать спецсредства для негласного получения информации

В) Лицензировать свои виды деятельности

Г) Предоставлять услуги в области шифрования

16. Анализ и прогноз динамики внешней и внутренней ситуации на предприятии, определение целей организационных структур службы безопасности, выявление проблем на пути достижения основной цели – это

А) Кадровое проектирование

Б) Календарное управление

В) Руководство

Г) Стратегическое управление

17. Сотрудники этой группы участвуют в обеспечении безопасности деятельности объекта с помощью технических средств защиты

А) Детективная группа

Б) Группа сопровождения

В) Техническая группа

Г) Группа безопасности

18. При организационном проектировании деятельности СБ предприятия первым этапом является:

А) Проектирование управленческой деятельности

Б) Формулирование целей и задач системы управления

В) Анализ и прогноз внешней ситуации

Г) Расчет экономической эффективности

Д) Решение основных вопросов формирования

19. Эта специализированная группа разрабатывает и проводит специальные мероприятия по изучению отдельных лиц из числа персонала объекта, посетителей и клиентов фирмы и жителей ближайшего к объекту окружения, в действиях которых содержатся угрозы безопасности деятельности объекта.

А) Группа сектора охранной безопасности

Б) Специализированная группа подбора

В) Детективная группа

Г) Группа внешних расследования

20. Техническая группа:

А) Работает совместно с группой охраны

Б) Отвечает за бесперебойную работу всех технических средств системы защиты объекта, ремонтирует и настраивает аппаратуру защиты

В) проверяют кандидатов для приема на работу на объекте;

Г) по отдельным заданиям руководства разрабатывают и проводят специальные мероприятия в отношении фирм-конкурентов;

21. Что самое главное должно продумать руководство при классификации данных?

А. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

Б Необходимый уровень доступности, целостности и конфиденциальности

В Оценить уровень риска и отменить контрмеры

Г Управление доступом, которое должно защищать данные

22. Безопасность информации – это

А) Совокупность мероприятий,

направленных на обеспечение конфиденциальности и целостности обрабатываемой информации, а также ее доступности для пользователей

Б) Такое ее состояние, при котором исключается возможность ознакомления с этой информацией, ее изменения или уничтожения лицами, не имеющими на это права;

В)Такое ее состояние, при котором исключается возможность ее утечки за счет ПЭМИ и наводок, специальных устройств перехвата

при передаче между объектами вычислительной техники

Г) А и Б

Д) Б и В

23. Информационная безопасность РФ – это

состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности и государства.

интересы государства создать условия для гармоничного развития, реализации конституционных прав и свобод человека и гражданина в конфиденциальности получения информации;

интересы государства и прав человека в доступе информации, не запрещенной законом;

защита информационных ресурсов от несанкционированного доступа

24. Кто является основным ответственным за определение уровня классификации информации?

А. Руководитель среднего звена

Б Высшее руководство

В Владелец

Г Пользователь

25. Как называется информация, к которой ограничен доступ?

А) *Конфиденциальная*

Б) Противозаконная

В) Открытая

Г) Недоступная

26. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

А)уязвимость информации

Б)надежность информации

В)защищенность информации

Г) *безопасность информации*

27. **Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это**

А)аудит

Б)*аутентификация*

В)авторизация

Г) идентификация

28. Основу политики безопасности составляет

А)программное обеспечение

Б)управление рисками

В)способ управления доступом

Г) выбор каналов связи

29. Первым этапом разработки системы защиты ИС является

А)*анализ потенциально возможных угроз*

Б)изучение информационных потоков

В)стандартизация программного обеспечения

Г) оценка возможных потерь

30. **Из перечисленного: 1) степень прогнозируемости; 2) природа происхождения; 3) предпосылки появления; 4) источники угроз; 5) размер ущерба — параметрами классификации угроз безопасности информации являются**

А)1,5

Б)3,4,5

В)*2,3,4*

Г) 1,2,3

Часть Б Задания репродуктивного уровня (выполнение деятельности по образцу, инструкции)

Вариант №1

Проведите сравнительный анализ инфракрасных датчиков движения

Вариант №2

Проведите сравнительный анализ ультразвуковых датчиков движения

Вариант №3

Проведите сравнительный анализ антивирусных программ

Вариант №4

Проведите сравнительный анализ межсетевых экранов

Вариант №5

Проведите сравнительный анализ аналоговых прямоугольных видеокамер

Вариант №6

Проведите сравнительный анализ аналоговых цилиндрических видеокамер уличного представления

Вариант №7

Проведите сравнительный анализ аналоговых купольных видеокамер для установки на потолок

Вариант №8

Проведите сравнительный анализ аналоговых поворотных видеокамер для максимального захвата территории объективом камеры

Вариант №9

Проведите сравнительный анализ аналоговых кубических видеокамер

Вариант №10

Проведите сравнительный анализ цифровых проводных корпусных видеокамер

Вариант №11

Проведите сравнительный анализ цифровых проводных поворотных видеокамер

Вариант №12

Проведите сравнительный анализ цифровых проводных купольных видеокамер

Вариант №13

Проведите сравнительный анализ цифровых проводных мини-камер видеонаблюдения

Вариант №14

Проведите сравнительный анализ беспроводных или IP видеокамер

Вариант №15

Проведите сравнительный анализ тепловых пожарных извещателей

Вариант №16

Проведите сравнительный анализ дымовых пожарных извещателей

Вариант №17

Проведите сравнительный анализ пламенных пожарных извещателей

Вариант №18

Проведите сравнительный анализ газовых пожарных извещателей

Вариант №19

Проведите сравнительный анализ комбинированных пожарных извещателей

Вариант №20

Проведите сравнительный анализ ручных пожарных извещателей

Вариант №21

Проведите сравнительный анализ ударно контактных извещателей

Вариант №22

Проведите сравнительный анализ пьезоэлектрических извещателей

Вариант №23

Проведите сравнительный анализ акустических извещателей разрушения стекла

Часть В Задания продуктивного уровня (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

Задача №1

Вы – ценный специалист медицинского центра, владеющий информационными технологиями. Вам необходимо выбрать медицинскую информационную систему, которая будет обеспечивать функционирование всего учреждения.

Выберите необходимый интерфейс информационной системы: «унифицированный» или «нестандартный».

Поясните ваш выбор руководителю (письменно).

Ответ к задаче №1

Унифицированный.

Унифицированный – стандартизированный. Правилом хорошего тона считается использование «мыши» и графического режима вывода изображения. Классическим примером унифицированного программного интерфейса является интерфейс программных продуктов фирмы Microsoft – MicrosoftWindows и MicrosoftOffice. Программы, обладающие унифицированным интерфейсом, как правило, легки в освоении и использовании.

Задача №2

Вы получили новый компьютер со склада. Компьютер предназначен для работы с документацией (электронного документооборота на предприятии нет) и для доступа в Интернет.

Какой минимальный набор программ вы установите?

Приведите примеры программ, которые распространяются бесплатно или условно бесплатно (свободное программное обеспечение).

Ответ к задаче №2

Операционная система, драйверы на устройства компьютера, офисный пакет, интернет-браузер (идет в комплекте с операционной системой), антивирусная программа, программа-архиватор

Операционная система (Linux), офисный пакет (OpenOffice), интернет-браузер (Mozilla, Chrome, Safari, IE, Opera), антивирусная программа (Avast, AVG), программа-архиватор (7-Zip, IZArc, TUGZip).

Задача №3

Вы заметили, что ваш ПК начал выполнять операции, команды на которые вы ему не отдавали: перезагружаться, запускать какие-то программы и т.д.

В чем может быть причина возникновения таких эффектов?

Как исправить данную ситуацию?

Ответ к задаче №3

Причиной такого поведения в большинстве случаев является вредоносное ПО – вирусы. Они загружаются в память вашего компьютера и выполняют действия, направленные на нарушение нормального процесса работы ПК.

Если у вас не установлен антивирусный пакет программ, то первейшим действием будет установка специального ПО для борьбы с вирусами и проверка компьютера. Если антивирус установлен, то необходимо обновить антивирусные базы, поскольку «пропущенный» вирус очевидно новее, чем последние антивирусные записи в вашей базе. После обновления баз следует также произвести полную проверку компьютера на вирусы.

Задача №4

На вашем компьютере хранится база данных о ваших коллегах: их персональные данные, электронные журналы и статьи. В последнее время вы заметили, что доступ к этой информации замедлился.

В чем может быть причина замедления доступа к информации?

Какое сервисное программное обеспечение следует применить, чтобы устранить проблему?

Ответ к задаче №4

Причина может заключаться в фрагментации диска (фрагментация диска - разбиение файла на диск при записи, при которой фрагменты файла оказываются в различных частях физического носителя) и / или вредоносной программы (вирус, трояны, программы-шутки и т.д.).

Для устранения фрагментации диска нужно провести дефрагментацию диска (дефрагментация диска – процесс обновления и оптимизации логической структуры раздела диска с целью обеспечить хранение файлов в непрерывной области). Нужно совершить следующие действия: пуск - все программы – стандартные – служебные - дефрагментация диска. Для устранения вредоносной программы нужно установить антивирусное программное обеспечение (если его нет), обновить сигнатуры базы данных, имеющейся антивирусной программы или сменить антивирусное ПО.

Задача № 5

Вы хотите перенести на другой компьютер с помощью флеш-накопителя один файл, размер которого превышает емкость накопителя.

Ваши действия?

Причина такого эффекта?

Ответ к задаче №5

Для выполнения этой задачи необходимо уменьшить размер файла, то есть заархивировать его. Архиваторы – программы, позволяющие создавать и обрабатывать архивные копии файлов посредством алгоритмов сжатия. Полученные архивные файлы имеют меньший размер, чем оригиналы.

Такой эффект достигается путем удаления из файлов избыточной информации. Для распаковки архивного файла и приведения его к первоначальному состоянию применяются обратные алгоритмы.

Задача №6

Вы – сотрудник N- учреждения. Ежедневно в базе данных происходит накопление большого количества информации.

1. Перечислите возможные способы способом обеспечения целостности и предотвращения уничтожения данных.

2. Определите, каким способом Вам необходимо воспользоваться. Объясните почему.

Ответ к задаче №6

1. Резервное копирование, архивирование.

2. В случае резервного копирования речь идет о кратко- или среднесрочном дополнительном хранении данных, которые еще могут понадобиться пользователям в их работе. Если, например, в результате повреждения жесткого диска или по иным причинам текущие данные теряются, их удастся быстро восстановить. Так можно эффективно защитить данные от разного рода случайностей. Время хранения резервных копий массива данных устанавливается не слишком продолжительное — несколько недель или месяцев.

Архивированию, напротив, подвергаются данные, которые из категории активно используемых перешли в «статичное» состояние, поэтому к ним обращаются сравнительно редко. Их можно уже извлечь из резервной копии и сохранить в архиве. Оба подхода различаются и уровнем затрат на приобретение необходимых технических средств: для архивирования большого объема данных применяются, как правило, недорогие носители с высокой емкостью хранения, например, оптические носители.

В описанной выше ситуации необходимо осуществлять резервное копирование данных.

Задача №7

На доске объявлений размещено сообщение, в котором говорится о том, что каждому сотруднику организации выделяется персональный пароль. Для того чтобы сотрудники его не забыли, пароль представляет дату рождения и имя каждого сотрудника.

1. Какие правила обеспечения информационной безопасности нарушены?

2. Какие символы должны быть использованы при записи пароля?

Ответ к задаче №7

1. Запрещается использовать в качестве пароля «пустой» пароль, имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а так же имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе.

Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах.

Запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем)

2. В качестве пароля должна выбираться последовательность символов, обеспечивающая малую вероятность её угадывания. Пароль должен легко запоминаться.

Задача №8

Вы – начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный

доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации.

1. Какая статья уголовного кодекса была нарушена?

2. Какое наказание должен понести нарушитель?

Ответ к задаче №8

1. Статья 272. Неправомерный доступ к компьютерной информации.

2. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, - наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Задача №9

Вы – руководитель отдела информационной безопасности организации. Вы подозреваете, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

1. Какая статья уголовного кодекса была нарушена?

2. Какое наказание должен понести нарушитель?

Ответ к задаче №9

1. Статья 273. Создание, использование и распространение вредоносных программ для ЭВМ.

2. Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами - наказываются лишением свободы на срок до трех лет со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев. Те же деяния, повлекшие по неосторожности тяжкие последствия, - наказываются лишением свободы на срок от трех до семи лет.

Задача №10

Гражданин П. проник в информационную базу ККБ и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.

Являются ли его действия противозаконными?

С чем это связано?

Какое наказание может ждать гражданина П. за совершенные им действия?

Ответ к задаче №10:

Да.

Гражданин П. нарушил закон – Гл.28 УК РФ ст. 272 Неправомерный доступ к компьютерной информации.

Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

Задача №11

По электронной почте Вам пришло сообщение, с прикрепленной к нему картинкой:

Содержит ли для Вас данное сообщение информацию? Для кого данное сообщение может содержать какую любо информацию? Почему?

Что понимают под термином «информация» применительно к компьютерной обработке данных?

Ответ к задаче № 11

Одно и то же информационное сообщение (статья в газете, объявление, письмо, телеграмма, справка, рассказ, чертёж, радиопередача и т.п.) может содержать разное количество информации для разных людей — в зависимости от их предшествующих знаний, от уровня понимания этого сообщения и интереса к нему.

Так как сообщение составлено на японском языке, то для Вас оно не несёт никакой информации как для человека, не знающего этого языка. Но это же сообщение может быть высокоинформативным для человека, владеющего японским.

Применительно к компьютерной обработке данных под «информацией» понимают некоторую последовательность символических обозначений (букв, цифр, закодированных графических образов и звуков и т.п.), несущую смысловую нагрузку и представленную в понятном компьютеру виде. Каждый новый символ в такой последовательности символов увеличивает информационный объём сообщения.

Задача №12

П.А. Андреев, сотрудник одного из филиалов ИТ-банка, внедрил в компьютерную банковскую систему вирус, уничтожающий исполняемые файлы (расширение .exe). В результате внедрения этого вируса было

уничтожено 40% банковских программных приложений, что принесло банку материальный ущерб в размере 750 000 рублей.

Какая статья УК РФ была нарушена?

Что послужило предметом преступления?

Какие неправомерные информационные действия были совершены А.П. Андреевым?

Ответ к задаче № 12

В данном случае совершено деяние, попадающее под действия ст. 273 УК РФ.

Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информациииили нейтрализации средств защиты компьютерной информации, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Основной объект преступления - общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Общественная опасность данного преступления определяется тем, что вредоносные программы способны парализовать работу компьютерной системы, а это может привести к неблагоприятным и даже катастрофическим последствиям.

Дополнительный объект преступления (ч. 3 ст. 273 УК РФ) - общественные отношения, обеспечивающие в зависимости от характера последних иные значимые социальные ценности (жизнь человека, здоровье многих людей, собственную безопасность и т.п.).

Предмет преступления по содержанию совпадает с предметом преступления, предусмотренного ст. 272 УК РФ.

Объективная сторона преступления включает альтернативные действия, состоящие: а) в создании компьютерных программ либо иной компьютерной

информации, заведомо способных приводить к несанкционированному уничтожению, блокированию, модификации, копированию компьютерной информации или нейтрализации средств защиты компьютерной информации; б) использовании компьютерных программ либо иной компьютерной информации; в) распространении таких программ либо иной компьютерной информации.

Предметом преступления является компьютерная информация, ограниченного доступа, т.е. сведения (сообщения, данные) независимо от формы их представления.

Неправомерное действие состоит в использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации.

3. ПАКЕТ ЭКЗАМЕНАТОРА

Помещение: Компьютерный класс

Оборудование: компьютеры объединенные в локальную сетьс выходом в интернет

Программное обеспечение: программа контроля знаний Nettest,пакетMicrosoftoffice, браузерInternetexplorer

Критерии оценки часть А:

Каждый правильный ответ на тестовое задание оценивается в 1 балл

Результат сумма баллов	Качественная оценка теоретической части	
	оценка	Вербальный аналог
27-30	5	Отлично
23-26	4	Хорошо
19-22	3	Удовлетворительно
18 и менее	2	Не удовлетворительно

Критерии оценки часть Б:

Результат сумма баллов	Качественная оценка теоретической части		Критерии выполнения практического задания
	оценка	Вербальный аналог	
27-30	5	Отлично	Практическое задание выполнено, верно, и в полном объеме согласно предъявляемым требованиям. Проанализированы ситуации, верно, сделаны аргументированные выводы. Дает ответы на дополнительные вопросы
23-26	4	Хорошо	Практическое задание выполнено, верно, и в полном объеме с пояснением всех действий. Произведен частичный анализ и (или) сделаны неверные выводы. Допущены недочеты
19-22	3	Удовлетвори тельно	Практическое задание выполнено наполовину, но без ошибок. Приведена недостаточно убедительная аргументация выполненного задания. Нарушена логика выполнения задания. Показаны недостаточные знания изучаемой дисциплины. Допущены несущественные ошибки
18 и менее	2	Не удовлетвори тельно	Практическое задание выполнено, но абсолютно неверно.

Критерии оценки часть В**:**

- оценка ***«отлично»:*** ответ на вопрос задачи дан правильный. Объяснение хода ее решения подробное, последовательное, грамотное, с теоретическими обоснованиями (в т.ч. из лекционного курса), с необходимым схематическими изображениями и демонстрациями на анатомических препаратах, с правильным и свободным владением анатомической терминологией; ответы на дополнительные вопросы верные, четкие. (27-30 баллов)

- оценка ***«хорошо»*****:** ответ на вопрос задачи дан правильный. Объяснение хода ее решения подробное, но недостаточно логичное, с единичными ошибками в деталях, некоторыми затруднениями в теоретическом обосновании (в т.ч. из лекционного материала), в схематических изображениях и демонстрациях на анатомических препаратах, ответы на дополнительные вопросы верные, но недостаточно четкие. (23-26 баллов)

- оценка ***«удовлетворительно»*****:** ответ на вопрос задачи дан правильный. Объяснение хода ее решения недостаточно полное, непоследовательное, с ошибками, слабым теоретическим обоснованием (в т.ч. лекционным материалом), со значительными затруднениями и ошибками в схематических изображениях и демонстрациях на анатомических препаратах, ответы на дополнительные вопросы недостаточно четкие, с ошибками в деталях. (19-22 балла)

- оценка ***«неудовлетворительно»*****:** ответ на вопрос задачи дан не правильный. Объяснение хода ее решения дано неполное, непоследовательное, с грубыми ошибками, без теоретического обоснования (в т.ч. лекционным материалом), без умения схематических изображений и демонстраций на анатомических препаратах или с большим количеством ошибок, ответы на дополнительные вопросы неправильные или отсутствуют. (18 и менее)