**Направление подготовки: 13.04.02–Электроэнергетика и электротехника**

**ПК-5. Способен применять методы и средства обеспечения информационной безопасности**

**Дисциплина «Кадровая безопасность предприятия»**

Прочитайте текст и выберите один правильный ответ

1. Наиболее опасной угрозой по кадровому направлению работы организаций, представляющих торговлю и сферу услуг, выступает
2. разглашение коммерческой тайны;
3. коррупция в форме взяток от поставщиков и подрядчиков;
4. прямые хищения имущества работодателя.

2. Для отечественных организаций работодателей наибольшую опасность представляют

1. угрозы в адрес собственного персонала;
2. угрозы со стороны собственного персонала;
3. угрозы со стороны нештатных сотрудников.
4. Основным законодательным инструментом обеспечения кадровой безопасности организаций – работодателей служит
5. Конституция РФ;
6. Уголовный кодекс РФ;
7. Трудовой кодекс РФ.
8. Затраты на эксплуатацию системы управления кадровой безопасностью организации должны быть
9. строго лимитированы;
10. соразмерны текущим финансовым возможностям организации;
11. соразмерны масштабам и вероятности ожидаемых угроз.
12. Общий контроль над соблюдением сотрудниками правил обеспечения информационной безопасности организации возложен
13. на руководителей структурных подразделений;
14. на службу безопасности;
15. на службу безопасности и на руководителей структурных подразделений.
16. Для обеспечения эффективного обучения сотрудников правилам обеспечения информационной безопасности руководителями структурных подразделений организации могут привлекаться специалисты
17. службы безопасности;
18. кадровой службы,
19. всех подразделений, работающих с конфиденциальной информацией.
20. Формирование стратегии управления кадровой безопасностью организации является задачей
21. службы персонала;
22. службы безопасности;
23. руководства компании.

8. Одной из причин внутренних угроз кадровой безопасности могут являться

1. алкогольная или наркотическая зависимость сотрудников;
2. сложная экономическая ситуация в регионе;
3. действующие федеральная и региональная нормативно-правовые базы.

9. К внутренним угрозам кадровой безопасности относятся

1. мошенничество, осуществляемое сотрудниками организации;
2. возможность оказания давления на сотрудников (подкуп, шантаж, провокации);
3. финансовые зависимости сотрудников организации от банков и других коммерческих структур.

10. К внешним угрозам кадровой безопасности можно отнести

1. угрозы в адрес руководителей компании со стороны криминальных структур;
2. умышленное повреждение оборудования работниками организации;
3. использование товарно-материальных ценностей в личных целях.

11. Наиболее распространенной сегодня группой методов защиты имущества организации от посягающих на него сотрудников выступают методы

1. технические;
2. организационные;
3. экономические.

12. Причиной большинства реализованных угроз имущественной безопасности со стороны собственных сотрудников организации является

1. злой умысел сотрудников;
2. их безответственность;
3. влияние на сотрудников со стороны конкурентов.

13. Профилактика угроз вербовки сотрудников организации начинается

1. на стадии испытательного срока;
2. после завершения испытательного срока;
3. на стадии отбора кандидатов на должность при трудоустройстве.

14. Конфиденциальные базы электронных данных предприятия наиболее целесообразно хранить

1. в компьютерах, отключенных от сети Интернет;
2. в компьютерах, отключенных от любой сети;
3. в компьютерах, отключенных от любой сети и размещенных в ограниченных для доступа помещений.

15. При ранжировании задач в рамках системы управления кадровой безопасностью организации должен обеспечиваться принцип приоритетности

1. мероприятий по эффективному отражению потенциальных угроз;
2. мероприятий по предотвращению потенциальных угроз;
3. мероприятий по выявлению и наказанию субъектов реализованных угроз.

16. При ранжировании задач в рамках системы управления кадровой безопасностью организации должен обеспечиваться принцип приоритетности защиты

1. высоколиквидных активов организации;
2. сотрудников организации;
3. конфиденциальной информации.

17. Установите соответствие между основными понятиями и их определением

|  |  |
| --- | --- |
| **Название** | **Определение** |
| А. Безопасность кадров | 1. Состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства. |
| Б. Кадровая безопасность | 1. Защищенность активов предприятия от угроз, исходящих от самого персонала предприятия (хищения, уничтожение или порча оборудования, сырья и другого имущества, оказание помощи конкурентам с использованием ресурсов предприятия и т. п.). |
| В. Информационная безопасность. | 1. Защищенность персонала и работы с ним от угроз нанесения ущерба. |

Ответ:

|  |  |  |
| --- | --- | --- |
| А | Б | В |
|  |  |  |

18. Установите соответствие между основными источниками угроз и действием направленных на персонал предприятия

|  |  |
| --- | --- |
| **Источники угроз** | **Действия, направленные**  **на персонал предприятия** |
| А. Конкуренты | 1. Взяточничество, использование ресурсов предприятия, в корыстных целях. |
| Б. Криминальные структуры | 2. Захват контроля над предприятием, хищения и нанесение иного ущерба. |
| В. Государственные структуры | 3. Ведение деловой разведки, переманивание высококвалифицированных специалистов, дискредитация соперника в глазах партнеров и государства. |

Ответ:

|  |  |  |
| --- | --- | --- |
| А | Б | В |
|  |  |  |

19. Закончите определение понятия. Процесс, событие, явление и т. п., которые могут негативно повлиять на нормальное функционирование и развитие объекта защиты и нанести ущерб (убытки, экономические потери) – это

Ответ:\_\_\_\_\_\_\_\_\_

20. Дополните. Ключевой ресурс предприятия, приводящий в действие все другие ресурсы, задействованные в получении прибыли, который уязвим и должен быть надежно защищен – это

Ответ:\_\_\_\_\_\_\_\_\_

**Таблица правильных ответов**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ вопроса** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Правильный ответ** | 1 | 2 | 3 | 3 | 2 | 3 | 3 | 1 | 1 | 1 | 2 | 1 | 3 | 3 | 2 | 2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ вопроса** | 17 | 18 | 19 | 20 |
| **Правильный ответ** | 231 | 321 | угроза | персонал |

**Дисциплина «Безопасность объектов критической информационной инфраструктуры»**

Прочитайте текст и выберите один правильный ответ

1. Какой федеральный орган исполнительной власти ответственен за обеспечение безопасности критической информационной инфраструктуры Российской Федерации
2. ФСТЭК России;
3. ФСБ России;
4. ФСО России.
5. Кто проводит категорирование КИИ
6. ФСБ России;
7. ФСТЭК России;
8. Комиссия субъекта КИИ.
9. Кто не может являться субъектом КИИ
10. индивидуальный предприниматель;
11. физическое лицо;
12. государственное учреждение.
13. Значимость в каких сферах деятельности не рассматривается в перечне показателей критериев значимости объектов КИИ
14. энергетики;
15. культурная;
16. экологическая.
17. Итоговым документом комиссии по категорированию объекта КИИ является
18. акт категорирования;
19. политика информационной безопасности;
20. Устав организации.
21. Деятельность в каких сферах не является критической согласно ФЗ №  87 «О безопасности информационной инфраструктуры Российской Федерации»
22. здравоохранение;
23. наука;
24. пищевая промышленность.

7. Конфиденциальность информации это:

1. обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
2. принцип неразглашения информации, не предназначенной для открытого доступа;
3. свойство информации быть известной только доверенным лицам.

8. Банк данных угроз безопасности информации создаёт и ведёт:

1. ФСТЭК России;
2. ФСБ России;
3. Роскомнадзор.

9. Требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации утверждены:

1. ФСБ России.
2. ФСТЭК России.
3. Минкомсвязи России.

10. Основным законом о критической информационной инфраструктуре Российской Федерации является:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
2. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;
3. Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о безопасности информации».

11. Субъектами критической информационной инфраструктуры не являются:

1. российские юридические лица и (или) индивидуальные предприниматели;
2. государственные органы и государственные учреждения;
3. физические лица.

12. ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» определяет компьютерную атаку как:

1. атака, инициированная с компьютера на другой компьютер или веб-сайт с целью нарушения целостности, конфиденциальности или доступности информации;
2. целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты КИИ, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;
3. любое неправомерное воздействие на программные и (или) программно-аппаратные средства и информацию.

13. Категорирование объектов критической информационной инфраструктуры осуществляется в порядке, установленном:

1. внутренними распорядительными документами субъекта КИИ;
2. Федеральным законом от 07.07.2003 № 126-ФЗ «О связи»;
3. постановлением Правительства Российской Федерации от 08.02.2018 № 127.

14. Установленное количество категорий значимости объектов критической

информационной ифраструктуры:

1. 4 категории значимости;
2. 3 категории значимости;
3. 6 категорий значимости.

15. Уполномоченным федеральным органом исполнительной власти в сфере ГосСОПКА является:

1. ФСБ России;
2. ФСТЭК России;
3. Минкомсвязь России.

16. Определение категорий значимости объектов критической информационной инфраструктуры осуществляется на основании:

1. мотивированного решения федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
2. показателей критериев значимости объектов критической информационной инфраструктуры и их значений, утверждённых Правительством Российской Федерации
3. согласия федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

17. Установите соответствие между основными понятиями и их определением

|  |  |
| --- | --- |
| **Название** | **Определение** |
| А. Значимый объект КИИ РФ | 1. Состояние защищенности информационных ресурсов (информационной среды) от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства. |
| Б. Безопасность кадров | 2. Объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры |
| В. Информационная безопасность. | 3.Защищенность активов предприятия от угроз, исходящих от самого персонала предприятия (хи-щения, уничтожение или порча оборудования, сы-рья и другого имущества, оказание помощи кон-курентам с использованием ресурсов предприятия и т. п.). |

Ответ:

|  |  |  |
| --- | --- | --- |
| А | Б | В |
|  |  |  |

18. Установите соответствие между основными понятиями и их определением

|  |  |
| --- | --- |
| **Название** | **Определение** |
| А. Информационная система | 1. Факт нарушения и прекращения функционирования объекта КИИ, сети электросвязи, используемой для организации взаимодействия таких объектов, и нарушения безопасности обрабатываемой таким объектом информации |
| Б. Компьютерный инцидент | 2. Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств |
| В.Информационно-телекоммуникационная сеть | 3.Технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники |

Ответ:

|  |  |  |
| --- | --- | --- |
| А | Б | В |
|  |  |  |

Закончите определение понятия -1 слово

19. Процедура, проверяющая, имеет ли пользователь с предъявленным идентификатором право на доступ к ресурсу – это…

Ответ:\_\_\_\_\_\_\_\_\_

Закончите определение понятия – 1 слово

20. Процесс, а также результат процесса проверки некоторых обязательных параметров пользователя и, при успешности, предоставление ему определённых полномочий на выполнение некоторых (разрешенных ему) действий в системах с ограниченным доступом – это …

Ответ:\_\_\_\_\_\_\_\_\_

**Таблица правильных ответов**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ вопроса** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Правильный ответ** | 1 | 3 | 2 | 2 | 1 | 3 | 1 | 1 | 1 | 1 | 3 | 2 | 3 | 2 | 1 | 2 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ вопроса** | 17 | 18 | 19 | 20 |
| **Правильный ответ** | 231 | 213 | Аутентификация | Авториза́ция |

**Преддипломная практика**

1. Основным законодательным инструментом обеспечения кадровой безопасности организаций – работодателей служит
2. Конституция РФ;
3. Уголовный кодекс РФ;
4. Трудовой кодекс РФ.
5. Затраты на эксплуатацию системы управления кадровой безопасностью организации должны быть
6. строго лимитированы;
7. соразмерны текущим финансовым возможностям организации;
8. соразмерны масштабам и вероятности ожидаемых угроз.
9. Общий контроль над соблюдением сотрудниками правил обеспечения информационной безопасности организации возложен
10. на руководителей структурных подразделений;
11. на службу безопасности;
12. на службу безопасности и на руководителей структурных подразделений.
13. Для обеспечения эффективного обучения сотрудников правилам обеспечения информационной безопасности руководителями структурных подразделений организации могут привлекаться специалисты
14. службы безопасности;
15. кадровой службы,
16. всех подразделений, работающих с конфиденциальной информацией.
17. Формирование стратегии управления кадровой безопасностью организации является задачей
18. службы персонала;
19. службы безопасности;
20. руководства компании.

6. Конфиденциальность информации это:

1. обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;
2. принцип неразглашения информации, не предназначенной для открытого доступа;
3. свойство информации быть известной только доверенным лицам.

7. Банк данных угроз безопасности информации создаёт и ведёт:

1. ФСТЭК России;
2. ФСБ России;
3. Роскомнадзор.

8. Требования о защите информации, связанные с применением криптографических методов защиты информации и шифровальных (криптографических) средств защиты информации утверждены:

1. ФСБ России.
2. ФСТЭК России.
3. Минкомсвязи России.

9. Основным законом о критической информационной инфраструктуре Российской Федерации является:

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
2. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»;
3. Федеральный закон от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и о безопасности информации».

10. Субъектами критической информационной инфраструктуры не являются:

1. российские юридические лица и (или) индивидуальные предприниматели;
2. государственные органы и государственные учреждения;
3. физические лица.

**Таблица правильных ответов**

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **№ вопроса** |  |  |  |  |  |  |  |  |  |  |
| **Правильный ответ** | 3 | 3 | 2 | 3 | 3 | 1 | 1 | 1 | 1 | 3 |

**Подготовка к процедуре защиты и защита выпускной квалификационной работы**

1. Итоговым документом комиссии по категорированию объекта КИИ является
2. акт категорирования;
3. политика информационной безопасности;
4. Устав организации.
5. Деятельность в каких сферах не является критической согласно ФЗ №  87 «О безопасности информационной инфраструктуры Российской Федерации»
6. здравоохранение;
7. наука;
8. пищевая промышленность.

**Таблица правильных ответов**

|  |  |  |
| --- | --- | --- |
| **№ вопроса** |  |  |
| **Правильный ответ** | 1 | 3 |