Министерство образования, науки и молодежной политики Нижегородской области

Государственное бюджетное профессиональное образовательное учреждение
«НИЖЕГОРОДСКИЙ ПРОМЫШЛЕННО-ТЕХНОЛОГИЧЕКИЙ ТЕХНИКУМ»

КОМПЛЕКТ КОНТРОЛЬНО ОЦЕНОЧНЫХ СРЕДСТВ

Учебной дисциплины

ОП.19 Основы информационной безопасности в органах внутренних дел

специальность
40.02.02 «Правоохранительная деятельность»

Нижний Новгород
2023г.

Контрольно - оценочные средства по учебной дисциплине «ОП.19 Основы информационной безопасности в органах внутренних дел» разработаны на основе ФГОС СПО по специальности: 40.02.02 Правоохранительная деятельность, утвержденного приказом Министерства образования и науки Российской Федерации от 12 мая 2014 г. № 509 и рабочей программы по дисциплине «ОП.19 Основы информационной безопасности в органах внутренних дел».

Организация-разработчик:
ГБПОУ «Нижегородский промышленно-технологический техникум»

Содержание

I. Паспорт комплекта контрольно-оценочных средств.

1. Общие положения

Контрольно-оценочные средства (КОС) разработаны в соответствии с требованиями основной профессиональной образовательной программы (ОПОП) и Федерального государственного стандарта по специальности 40.02.02 Правоохранительная деятельность среднего профессионального образования (СПО), программы учебной дисциплины «ОП.19 Основы информационной безопасности в органах внутренних дел».

Контрольно-оценочные средства предназначены для контроля и оценки образовательных достижений обучающихся, освоивших программу учебной дисциплины «ОП.19 Основы информационной безопасности в органах внутренних дел» для специальности СПО 40.02.02 Правоохранительная деятельность.

КОС включают контрольные материалы для проведения текущего контроля и промежуточной аттестации в форме экзамена.

2. Результаты освоения учебной дисциплины, подлежащие проверке

Комплект контрольно-оценочных средств предназначен для проверки уровня усвоения учебной дисциплины «ОП.19 Основы информационной безопасности в органах внутренних дел». Освоение содержания учебной дисциплины «ОП.19 Основы информационной безопасности в органах внутренних дел» обеспечивает достижение студентами следующих результатов:

Результаты обучения (освоенные умения, усвоенные знания)	**Формы и методы контроля и оценки результатов обучения**
В результате освоения дисциплины обучающийся должен уметь:	**Формы контроля обучения:**
- практически оценивать риски, связанные с ситуациями несанкционированного доступа к информации, злоумышленной модификации информации и утраты служебной информации; - предотвращать в служебной деятельности ситуации, связанные с информационными рисками; - формулировать проблемы для их решения специалистами служб безопасности и защиты информации; - использовать программно-аппаратные и технические средства защиты информации; - применять программно-аппаратные средства при аутентификации электронных документов с использованием электронной цифровой подписи.	Текущий контроль: устный опрос, письменное тестирование; самостоятельная работа, практические задания, активность на занятиях. Промежуточный контроль: - экзамен.

В результате освоения дисциплины обучающийся должен знать:	
- сущность и содержание основных понятий в сферах информационной безопасности и зашиты информации; - основные положения Концепции национальной безопасности России и Доктрины информационной безопасности России; - главные положения законодательства России и ведомственных нормативных правовых актов в сфере информационных отношении: - сущность и основные каналы утечки информации на объектах информатизации ОВД; - основные методы и способы зашиты информационных процессов в компьютерных системах: - основные методы и способы защиты информации в телекоммуникационных системах (Интернет, ЕИТКС ОВД).	Текущий контроль: устный опрос, письменное тестирование; самостоятельная работа, практические задания, активность на занятиях. Промежуточный контроль: - экзамен.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся сформированность профессиональных компетенций.

Результаты обучения (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.2 Обеспечивать соблюдение законодательства субъектами права.	Демонстрирует правильность формирования профессиональных навыков по выявлению нарушений соблюдения законодательства Российской Федерации субъектами права; осуществляет отбор, и систематизацию законоположений, относящихся к ситуациям, нуждающимся в правовой оценке и регулировании; решает ситуации, связанные с соблюдением законодательства Российской Федерации субъектами права.	Текущий контроль в форме: - фронтального опроса; - практических занятий; - тестового задания по темам; - решение ситуационных задач по теме. Промежуточный контроль: - экзамен.
ПК 1.10. Использовать в профессиональной деятельности нормативные	Демонстрирует знание основных законов и нормативных правовых	Текущий контроль в форме: - фронтального опроса;

правовые акты и документы по обеспечению режима секретности в Российской Федерации.	актов, регламентирующих деятельность органов внутренних дел, регламентирующих обеспечение режима секретности. Умеет правильно составлять и оформлять служебные документы, в том числе секретные, содержащие сведения ограниченного пользования.	- практических занятий; - тестового задания по темам; - решение ситуационных задач по теме. Промежуточный контроль: - экзамен.
ПК 1.11. Обеспечивать защиту сведений, составляющих государственную тайну, сведений конфиденциального характера и иных охраняемых законом тайн.	Демонстрирует знание основных законов и нормативных правовых актов, регламентирующих деятельность органов внутренних дел, регламентирующих защиту сведений составляющих государственную тайну, служебную тайну. Умеет правильно составлять и оформлять служебные документы, в том числе секретные, содержащие сведения ограниченного пользования; а также выполнять служебные обязанности в строгом соответствии с требованиями режима секретности.	Текущий контроль в форме: - фронтального опроса; - практических занятий; - тестового задания по темам; - решение ситуационных задач по теме. Промежуточный контроль: - экзамен.

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся не только сформированность профессиональных компетенций, но и развитие общих компетенций и обеспечивающих их умений.

Результаты обучения (освоенные общие компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ОК 1. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес.	Демонстрирует устойчивый интерес к будущей профессии; владеет приемами совершенствования профессиональных знаний и профессионального опыта.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.

ОК 3. Организовывать собственную деятельность, выбирать типовые методы и способы выполнения профессиональных задач, оценивать их эффективность и качество.	Знает наиболее эффективное обоснование выбора и наиболее актуальные методы, и способы решения профессиональных задач в области информационной безопасности; Умеет наиболее эффективно организовать свою учебно-практическую деятельность в разрешении тех или иных правовых ситуаций, при выполнении поставленных задач.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.
ОК 4. Принимать решения в стандартных и нестандартных ситуациях, в том числе ситуациях риска, и нести за них ответственность.	Знает теоретическое обоснование и алгоритм действий, при принятии решений в ситуациях пограничных с чрезвычайными и ситуациями риска, в том числе в области информационной безопасности; Умеет правильно организовать деятельность по защите информации, соотносить свои возможности и как следствие понимать всю полноту ответственности.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.
ОК 6. Осуществлять поиск и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития.	Знает систему источников права и систему нормативно-правовых актов РФ в области информационной безопасности; Умеет ориентироваться в источниках права, умеет находить нужные нормы права в системе законодательства, для разрешения правовых ситуаций в области информационной безопасности.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.
ОК 7. Использовать информационно-коммуникационные технологии в профессиональной	Знает алгоритм работы с информационно-правовыми системами; Умеет демонстрировать навыки использования	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное

деятельности.	информационно- правовых систем (технологий) в профессиональной деятельности, а также эффективно использовать технологии защиты информации в органах внутренних дел.	выполнение самостоятельной работы, проверка результатов работы.
ОК 11. Самостоятельно определять задачи профессионального и личностного развития, заниматься самообразованием, осознанно планировать повышение квалификации.	Знает значение и роль повышения квалификации сотрудников системы правоохранительных органов, в том числе в области информационной безопасности. квалификации; Умеет организовать работу по самообразованию.	Практическое занятие. Проверка правильности выполнения практической работы. Своевременное выполнение самостоятельной работы, проверка результатов работы.

2. Задания для текущего контроля, критерии оценки, эталоны ответов

Тестирование

Тест.

1. Назовите Федеральный закон, который регулирует отношения, возникающие при обеспечении защиты информации:

а) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

в) Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

2. Как Федеральный закон Российской Федерации от 27 июля 2006 г. №149 подразделяет информацию в зависимости от категории доступа к ней:

а) на общедоступную информацию;

б) на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа);

в) на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Перечислите принципы, на которых основывается правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации:

а) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

б) установление ограничений доступа к информации только федеральными законами и решением руководителя;

в) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

г) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

д) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

е) достоверность информации и своевременность ее предоставления;

ж) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

з) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими.

4. Что такое конфиденциальность информации:

а) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

б) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без законодательно оформленного соглашения;
в) конфиденциальность информации - обязательное для выполнения лицом, получившим доступ копределенной информации, требование не передавать такую информацию третьим лицам без росписи в журнале посетителей о полученной информации.

5. Требованиями каких законов регулируется защита информации, составляющей государственную тайну:
а) Законом Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;
б) Указом президента Российской Федерации «О перечне сведений, отнесенных к государственной тайне»;
в) в соответствии с законодательством Российской Федерации о государственной тайне.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии:
а) с федеральными законами и (или) по решению суда;
б) с федеральными законами;
в) по решению суда.

7. Назовите виды информационных систем:
а) государственные информационные системы;
б) муниципальные информационные системы;
в) личные информационные системы.

8. Что представляет собой защита информации:
а) принятие правовых, организационных и технических мер;
б) принятие правовых и технических мер;
в) принятие правовых и организационных мер.

9. На что направлено принятие правовых, организационных, технических и экономических мер защиты информации:
а) на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
б) на соблюдение конфиденциальности информации ограниченного доступа;
в) на реализацию права на доступ к информации.

10. В каких случаях не требуется обеспечение конфиденциальности персональных данных:
а) в случае обезличивания персональных данных, а также в отношении общедоступных персональных данных;
б) в отношении общедоступных персональных данных;
в) в случае обезличивания персональных данных.

11. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Секретно»:

а) первая;
б) вторая;
в) третья.

12. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Сов. Секретно»:
а) первая;
б) вторая;
в) третья.

13. Какова должна быть категория объектов информатизации, на которых обрабатывается информация с грифом «Особой важности»:
а) первая;
б) вторая;
в) третья.

14. Назовите виды конфиденциальной информации, утвержденные Указом президента Российской Федерации «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188:
а) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях;
б) сведения, составляющие тайну следствия и судопроизводства;
в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);
г) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т. д.);
д) сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна);
е) сведения о стихийных бедствиях;
ж) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

15. Каким руководящим документом определены требования по порядку разработки и содержанию «Положения о подразделении (специалисте) по защите информации»:
а) Решением Гостехкомиссии России № 42 от 03.10.1995 г.;
б) Решением Гостехкомиссии России № 42 от 03.10.1995 г. и Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
в) Решением Гостехкомиссии России от 14.03.1995 № 32.

16. Каким руководящим документом определены требования по порядку разработки и содержанию «Руководства по защите информации...»:

а) Решением Гостехкомиссии России № 42 от 03.10.1995 г.;
б) Решением Гостехкомиссии России № 42 от 03.10.1995 г. и Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
в) Решением Гостехкомиссии России от 14.03.1995 № 32.

17. Каким руководящим (нормативно правовым) документом определены требования к содержанию и порядку определения политики безопасности предприятия:
а) Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
б) Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
в) Доктриной информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895;
г) никаким.

18. Сколько существует классов защищенности АС от несанкционированного доступа:
а) три;
б) пять;
в) семь;
г) девять.

19. На сколько групп разбиты классы защищенности АС от несанкционированного доступа:
а) на две;
б) на три;
в) на пять.

20. Основные способы НСД к информации:
а) непосредственное обращение к объектам доступа;
б) создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
в) модификация средств защиты, позволяющая осуществить НСД;
г) поиск необходимой информации по Интернету;
д) внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

21. Основными характеристиками технических средств защиты являются:
а) степень полноты охвата ПРД реализованной СРД и ее качество;
б) состав и качество обеспечивающих средств для СРД;
в) гарантии правильности функционирования СРД и обеспечивающих ее средств;
г) рейтинг производителя;
д) стоимость технических средств и качество эксплуатации.

22. Какие характеристики объектов и субъектов защиты должны быть положены в основу системы классификации АС:
а) информационные - определяющие ценность информации, ее объем и

степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования АС из-за искажения (потери) информации;
б) организационные - определяющие полномочия пользователей;
в) уровень образования сотрудников;
г) технологические - определяющие условия обработки информации (способ обработки, время циркуляции, вид АС).

23. Основные этапами классификации АС:
а) разработка и анализ исходных данных;
б) выявление основных признаков АС, необходимых для классификации;
в) сравнение выявленных признаков АС с классифицируемыми;
г) разработка матрицы доступа;
д) присвоение АС соответствующего класса защиты информации от НСД.

24. Необходимые исходные данные для проведения классификации конкретной АС:

а) перечень защищаемых информационных ресурсов АС и уровень их конфиденциальности;
б) перечень лиц, имеющих доступ к штатным средствам АС, с указанием уровня их полномочий;
в) матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
г) наличие инструкции пользователю;
д) режим обработки данных в АС.

25. Что относят к числу определяющих признаков, по которым производится группировка АС в различные классы:
а) наличие в АС информации различного уровня конфиденциальности;
б) уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
в) наличие приказа по организации об установлении класса защищенности АС;
г) режим обработки данных в АС: коллективный или индивидуальный.

26. Из каких подсистем условно состоит в общем случае комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД в рамках системы защиты информации от НСД ИСПДн:
а) управления доступом;
б) регистрации и учета;
в) криптографической;
г) мониторинга вторжений;
д) обеспечения целостности;
е) круглосуточного видеонаблюдения;
ж) антивирусной.

27. Из каких подсистем условно состоит в общем случае комплекс программно-технических средств и организационных решений (процедурных) по защите информации от НСД в рамках системы защиты информации в АС:
а) управления доступом;
б) регистрации и учета;
в) круглосуточного видеонаблюдения;
г) криптографической;
д) обеспечения целостности;
28. Типовая структура службы безопасности:
а) отдел режима и охраны, в составе сектора режима и сектора охраны;
б) отдел защиты информации;
в) группа бухгалтерского учета;
г) инженерно-техническая группа;
д) группа безопасности внешней деятельности.
29. Основные документы, регламентирующие деятельность подразделения (специалиста) по защите информации:
а) Конституция Российской Федерации;
б) Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
в) Положение о подразделении (специалисте) по защите информации;
г) Решением Гостехкомиссии России от 14.03.1995 № 42.
30. Какой основной нормативно-правовой акт должен быть оформлен сотруднику перед допуском его к работе с информацией ГТ с грифом совершенно секретно:
а) трудовой договор;
б) дополнение к трудовому договору;
в) форма допуска №3.
31. Какой основной нормативно-правовой акт должен быть оформлен сотруднику перед допуском его к работе с информацией ГТ с грифом совершенно секретно:
а) приказ по организации о процентной надбавки за секретность;
б) должностная инструкция;
в) форма допуска №2.
32. Кто оформляет форму допуска №3:
а) Руководитель территориального Управления ФСТЭК по федеральному округу;
б) Руководитель организации;
в) Территориальный орган ФСБ России.
33. Кто оформляет форму допуска №2:
а) Руководитель территориального Управления ФСТЭК по федеральному округу;
б) Руководитель организации;
в) Территориальный орган ФСБ России.
34. Сколько классов защищенности ИСПДн от НСД:

а) три;
б) четыре;
в) пять.

35. Доктрина информационной безопасности Российской Федерации

представляет собой совокупность официальных взглядов на:
а) цели
б) взгляды
в) задачи
г) принципы

36. Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных:
а) угрозах
б) интересов личности
в) общества
г) государства

37. Источники угроз информационной безопасности Российской Федерации подразделяются на:
а) внешние
б) основные
в) внутренние

38. Успешному решению вопросов обеспечения информационной безопасности Российской Федерации способствуют системы:
а) государственная система защиты информации
б) система зашиты президента
в) система защиты государственной тайны
г) системы сертификации средств защиты информации

39. Общие методы обеспечения информационной безопасности Российской Федерации разделяются на:
а) экономические
б) внешние
в) правовые
г) организационно-технические

40. Наибольшую опасность в сфере внутренней политики представляют следующие угрозы информационной безопасности Российской Федерации:
а) нарушение конституционных прав и свобод граждан
б) распространение дезинформации о политике РФ
в) деятельность общественных объединений, направленная на насильственное изменение основ конституционного строя и нарушение целостности РФ
г) мероприятиями в области обеспечения информационной безопасности РФ

41. Основными направлениями обеспечения информационной безопасности Российской Федерации в сфере духовной жизни являются:
а) распространение дезинформации о политике РФ

б) развитие в России основ гражданского общества
в) государственная поддержка мероприятий по сохранению и возрождению культурного наследия народов и народностей РФ
г) противодействие негативному влиянию иностранных религиозных организаций и миссионеров.

42. Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются
а) запрещение разработки, распространения и применения "информационного оружия”
б) обеспечение безопасности международного информационного обмена
в) обеспечение безопасности для торговли людьми
г) предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях

43. Государственная политика обеспечения информационной безопасности РФ основывается на следующих основных принципах:
а) соблюдение Конституции РФ, законодательства РФ, общепризнанных принципов и норм международного права
б) правовое равенство всех участников процесса информационного взаимодействия вне зависимости от их политического, социального и экономического статуса
в) соблюдении правил дорожного движения
г) приоритетное развитие отечественных современных информационных и телекоммуникационных технологий

44. Г осударство в процессе реализации своих функций по обеспечению информационной безопасности Российской Федерации:
а) обеспечивает безопасность интересов граждан
б) проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности РФ, разрабатывает меры по ее обеспечению
в) проводит необходимую протекционистскую политику в отношении производителей средств информатизации и защиты информации на территории РФ
г) способствует интернационализации глобальных информационных сетей и систем

45. Первоочередными мероприятиями по реализации государственной политики обеспечения информационной безопасности Российской Федерации являются:
а) разработка и внедрение механизмов реализации правовых норм, регулирующих отношения в информационной сфере
б) развитие системы подготовки кадров, используемых в области обеспечения информационной безопасности РФ
в) гармонизация отечественных стандартов в области информатизации и обеспечения информационной безопасности автоматизированных систем управления
г) переход к рыночным отношениям в экономике

46. Основными функциями системы обеспечения информационной безопасности Российской Федерации являются:
а) создание условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере
б) обеспечение безопасности компьютерного пиратства
в) разработка нормативной правовой базы в области обеспечения информационной безопасности РФ
г) предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере
47. Компетенция федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов, входящих в состав системы обеспечения информационной безопасности РФ определяется:
а) федеральными законами
б) нормативными правовыми актами Президента РФ
в) Правительством РФ
г) компьютерным пиратством
48. Система обеспечения информационной безопасности Российской Федерации строится на основе разграничения полномочий органов:
а) законодательной власти
б) народной власти
в) исполнительной власти
г) судебной власти
49. Основными элементами организационной основы системы обеспечения информационной безопасности Российской Федерации являются:

а) принцип законности
б) Президент Российской Федерации
в) Совет Безопасности РФ
г) Государственная Дума Федерального Собрания РФ
50. Правовая база, регулирующая отношения, возникающие при обеспечении защиты информации:
Федеральный закон Российской Федерации от 27 июля 2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации»;
Федеральный закон Российской Федерации от 27 июля 2006 г. № 152- ФЗ «О персональных данных»;
Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.
51. Основные способы НСД к информации: непосредственное обращение к объектам доступа; создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты; поиск необходимой информации по сети Интернет; модификация средств защиты, позволяющая осуществить НСД; внедрение в технические средства СВТ или

АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

52. Виды информации в зависимости от категории доступа к ней согласно законодательства РФ делятся:

на общедоступную информацию;

на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа);

на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

53. Каким руководящим (нормативно правовым) документом определены требования к содержанию и порядку определения политики безопасности предприятия:

Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Доктриной информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895;

никаким.

54. Классы защищенности средств вычислительной техники от несанкционированного доступа.

три;

четыре;

пять.

55. Факторы, влияющие на требуемый уровень защиты информации. Гриф секретности;

Режим обработки информации;

Права пользователей.

56. Укажите основные законы, относящиеся к организации и функционированию системы информационной безопасности и защиты информации

Федеральный закон Российской Федерации от 27 июля 2006 г. № 149- ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152- ФЗ «О персональных данных»;

Доктрина информационной безопасности Российской Федерации от 9 сентября 2000 г. № Пр-1895.

57. Каковы основные отечественные и зарубежные стандарты в области информационной безопасности?

ISO 17799

ГОСТ Р ИСО/МЭК 15408;

ГОСТ Р 51241-98.

58. Что такое политика безопасности?

Свод правил предприятия по обеспечению информационной безопасности;

Мнение руководителя предприятия;
Должностные инструкции сотрудников.
58. Что такое государственная тайна?
Конфиденциальная информация;
Информация для служебного пользования;
Информация ограниченного распространения.
59. Что такое коммерческая тайна?
Конфиденциальная информация;
Информация для служебного пользования;
Информация ограниченного распространения.
60. Что такое служебная тайна?
Конфиденциальная информация;
Информация для служебного пользования;
Информация с грифом секретно.
61. Что такое профессиональная тайна?
Конфиденциальная информация;
Информация для служебного пользования;
Информация с грифом секреетно.
62. Что такое персональные данные?
Конфиденциальная информация;
Информация для служебного пользования;
Информация ограниченного распространения.
63. Что такое источники права на доступ к информации?
Правовая база РФ по безопасности информации;
Форма допуска сотрудника;
Решение руководителя организации.
64. Каковы уровни доступа к информации с точки зрения законодательства?
Форма допуска 1;
Форма допуска 2;
Форма допуска 5 Форма допуска 3.
65. Что такое информация ограниченного распространения?
Конфиденциальная информация;
Информация для служебного пользования;
Информация ограниченного распространения;
Государственная тайна.
66. Источники угроз?
Внешние источники угроз;
Служебные разногласия;
Внутренние источники угроз.
67. Что делает правительство РФ в пределах своих полномочий? Организует работы по защите информации;
Осуществляет методическое руководство;
Выполняет мероприятия по защите информации;
Осуществляет контроль
68. Что делает Совет Безопасности РФ?

Разрабатывает Концепцию национальной безопасности; Организует работы по защите информации;
Осуществляет методическое руководство;
Осуществляет контроль.

69. Что делают Федеральные органы исполнительной власти? Организуют работы по защите информации;
Осуществляют методическое руководство;
Осуществляют контроль

70. Что делают Межведомственные и государственные комиссии?
Организует работы по защите информации;
Осуществляет методическое руководство;
Осуществляет контроль

71. Что делают Органы исполнительной власти субъектов Российской Федерации?
Организуют работы по защите информации;
Осуществляют методическое руководство;
Осуществляют контроль;
Проводят работы по защите информации.

72. Что делают Органы местного самоуправления?
Организуют работы по защите информации;
Осуществляют методическое руководство в организациях (на предприятиях);
Осуществляют контроль

73. Что делают Органы судебной власти?
Организуют работы по защите информации;
Осуществляют методическое руководство;
Осуществляют контроль
Осуществляют прокурорский контроль и принимают решение о привлечении к ответственности за нарушения в области

информационной безопасности.

74. Модели нарушителей информационной безопасности на объекте.
Две;
Три;
Четыре.

75. Типовая структура службы безопасности.
отдел защиты информации;
отдел режима и охраны, в составе сектора режима и сектора охраны;
инженерно-техническая группа;
отдел по борьбе с националистическими проявлениями;
группа безопасности внешней деятельности.

Критерии оценки при проведении тестирования:

Отметка	Критерии оценки
«5»	*90-100 % правильных ответов*
«4»	*60-89% правильных ответов*
«3»	*50-59 % правильных ответов*
«2»	*Менее 50 % правильных ответов*

3. Задания для промежуточной аттестации, критерии оценки.

Промежуточная аттестация студентов проводится в форме устного экзамена. КОС предназначен для контроля и оценки результатов освоения учебной дисциплины ОП.19 Основы информационной безопасности в органах внутренних дел. Комплект материалов для оценки сформированности умений и знаний представлен в виде вопросов для подготовки к экзамену.

Примерный перечень экзаменационных вопросов по дисциплине «ОП.19 Основы информационной безопасности в органах внутренних дел»:

1. Что понимается под национальной безопасностью РФ?
2. В чем заключаются национальные интересы РФ?
3. Какими факторами обусловлены угрозы национальным интересам РФ в международной сфере?
4. Назовите важнейшие задачи обеспечения информационной безопасности РФ.
5. Как влияют процессы информатизации общества на содержание национальной безопасности?
6. Назовите основные угрозы конституционным правам и свободам человека и гражданина.
7. Назовите основные угрозы информационному обеспечению государственной политики РФ.
8. Назовите основные угрозы безопасности информационных и телекоммуникационных средств и систем.
9. Что представляют собой внешние и внутренние источники угроз информационной безопасности РФ?
10. В чем состоит государственная политика обеспечения информационной безопасности РФ?
11. Какие действия предпринимает государство по совершенствованию правовых механизмов в области обеспечения информационной безопасности РФ?
12. На каких принципах должно базироваться правовое обеспечение информационной безопасности РФ?
13. Что понимается под информационным оружием? Представьте его классификацию.
14. Назовите основные виды и объекты воздействия в информационной войне.
15. Назовите отличительные особенности информации как продукта.
16. Какую информацию относят к открытой, конфиденциальной, секретной?
17. Что включает понятие «государственная тайна»?
18. Какова структура государственной системы информационной безопасности?

19. Какими полномочиями наделена ФСТЭК России? Какие задачи в области обеспечения информационной безопасности она решает?
20. Какими полномочиями наделена ФСБ России? Какие задачи в области обеспечения информационной безопасности она решает?
21. Какие задачи призвана решать государственная система обеспечения информационной безопасности?
22. Назовите основные категории источников конфиденциальной информации в информационных системах.
23. Что понимается под способом несанкционированного доступа к источнику конфиденциальной информации?
24. Какие способы несанкционированного доступа к источнику конфиденциальной информации Вам известны?
25. Укажите угрозы конфиденциальной информации.
26. В чем состоит правовая защита конфиденциальной информации?
27. Какими законами Российской Федерации регламентируется охранная деятельность?
28. В каких целях в Российской Федерации проводится лицензирование отдельных видов деятельности?
29. Какие виды деятельности подлежат лицензированию в области технической защиты информации?
30. Какой порядок установлен для лицензирования деятельности по технической защите конфиденциальной информации?
31. С какой целью проводится аттестация информационной системы? Каков порядок проведения аттестации?
32. С какой целью проводится сертификация средств защиты информации по требованиям безопасности информации?
33. Каков порядок сертификации средств защиты информации?
34. Какой порядок установлен для сертификации средств защиты информации зарубежного производства?
35. Каковы особенности механизма закрепления права на интеллектуальную собственность?
36. Кто выступает в качестве объекта и субъекта информационных правоотношений в системе авторского права?
37. Каковы особенности правового регулирования авторского и имущественного права при производстве и распространении программ для ЭВМ и баз данных?
38. Как должны действовать правообладатели при защите своего права на интеллектуальную собственность?
39. Каков порядок правового регулирования информационных отношений при производстве и распространении топологий интегральных микросхем?
40. Каковы особенности регулирования информационных отношений институтом патентного права?
41. Что относится к объектам изобретения, полезным моделям, промышленным образцам?

42. Кто может стать автором изобретения, полезной модели, промышленного образца?
43. В чем заключается разница между автором и правообладателем?
44. Что относится к персональным данным? Укажите их особенности.
45. Какие функции выполняет оператор персональных данных?
46. Назовите основные принципы обработки персональных данных.
47. В чем состоят права субъекта персональных данных?
48. В чем состоят обязанности оператора при сборе и обработке персональных данных?
49. Какие санкции могут быть наложены на оператора, его руководителей и должностных лиц при нарушении законодательства о безопасности обработки персональных данных?
50. Назовите основные задачи Федеральных органов по контролю и надзору за соблюдением законодательства в области безопасности персональных данных.
51. Приведите примеры правонарушений в сфере компьютерной передачи информации.
52. Чем характеризуются признаки состава компьютерного преступления и из каких элементов оно может состоять?
53. В чем заключаются особенности расследования компьютерного преступления?
54. С какими факторами связаны проблемы судебного преследования за преступления в сфере компьютерной информации?
55. В чем заключается понятие международного информационного обмена.
56. Чем определяется правовой режим участия в международном обмене субъектов Российской Федерации?
57. Дайте краткую характеристику законодательству зарубежных стран в области защиты интеллектуальной собственности.
58. На чем основываются и чем характеризуются международные правовые аспекты защиты прав и свобод личности в связи с применением современных информационных технологий?
59. Какие примеры международного сотрудничества в области борьбы с преступностью в сфере информационных технологий Вам известны?

Критерии оценки:

Оценка	Критерии
«Отлично»	-студент раскрыл содержание материала в объеме, предусмотренном программой; -изложил материал грамотным языком в определенной логической последовательности, точно используя терминологию данного предмета как учебной дисциплины; -продемонстрировал усвоение ранее изученных сопутствующих вопросов, сформированность и устойчивость используемых при ответе умений и навыков;

	-отвечал самостоятельно без наводящих вопросов преподавателя. -- Возможны одна – две неточности при освещении второстепенных вопросов или в выкладках, которые студент легко исправил по замечанию преподавателя. -
«Хорошо»	-допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; -допущены ошибка или более двух недочетов при освещении второстепенных вопросов или в выкладках, легко исправленные по замечанию преподавателя.
«Удовлетворительно»	-неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала определенные настоящей программой -несоответствие выводов, сделанных экзаменующимся, толкованию норм законодательства; -своевременное исправление ошибок при изложении ответа.
«Неудовлетворительно»	- не раскрыто основное содержание учебного материала; -обнаружено незнание или неполное понимание учеником большей или наиболее важной части учебного материала; - допущены ошибки в определении понятий, при использовании специальной терминологии, которые не исправлены после нескольких наводящих вопросов преподавателя

4. Перечень информационных источников

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы

Нормативно-правовые акты:

Основная литература:

1. Суворова, Г. М. Основы информационной безопасности : учебное пособие для СПО / Г. М. Суворова. — Саратов : Профобразование, 2021. — 135 с. — ISBN 978-5-4488-1294-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS.

Дополнительная литература:

2. Гультяева, Т. А. Основы информационной безопасности : учебное пособие / Т. А. Гультяева. — Новосибирск : Новосибирский государственный технический университет, 2018. — 79 с. — ISBN 978-5-7782-3640-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.

3. Лапонина, О. Р. Основы сетевой безопасности: криптографические алгоритмы и протоколы взаимодействия : учебное пособие / О. Р. Лапонина ; под редакцией В. А. Сухомлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 605 с. — ISBN 978-5-4497-0684-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART.

Интернет-ресурсы:

www.fcior.edu.ru (Федеральный центр информационно-образовательных ресурсов — ФЦИОР).

www. school-collection.edu.ru (Единая коллекция цифровых образовательных ресурсов).

http://ru.iite.unesco.org/publications (Открытая электронная библиотека «ИИТО ЮНЕСКО» по ИКТ в образовании).

www.megabook.ru (Мегаэнциклопедия Кирилла и Мефодия, разделы «Наука / Математика. Кибернетика» и «Техника / Компьютеры и Интернет»).

www.ict. edu. ru (портал «Информационно-коммуникационные технологии в образовании»).

www.digital-edu.ru (Справочник образовательных ресурсов «Портал цифрового образования»).

www.window. edu. ru (Единое окно доступа к образовательным ресурсам Российской Федерации).