НЕГОСУДАРСТВЕННОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
«ЯКУТСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»
(НПОУ «ЯКИТ»)

Отделение информационных технологий

Специальность 40.02.02 Правоохранительная деятельность

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО

практическим занятиям

по дисциплине ОП.10 Организационно-правовое обеспечение информационной безопасности

г. Якутск, 2025 г.

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Настоящие методические рекомендации разработаны для организации и проведения практических занятий по дисциплине ОП.10 «Организационно-правовое обеспечение информационной безопасности» в соответствии с требованиями профессионального стандарта по специальности 40.02.02 Правоохранительная деятельность.

Цель практических занятий:

Основная цель практических занятий по данной дисциплине - формирование у обучающихся практических навыков и умений, необходимых для эффективного использования информационных технологий в их будущей профессиональной деятельности. Практические занятия направлены на закрепление теоретических знаний, полученных на лекциях, и их применение в решении конкретных профессиональных задач.

Методические рекомендации содержат:

1. Тематический план практических занятий в соответствии с рабочей программой дисциплины.
2. Подробное описание каждого практического занятия, включая цели, задачи, необходимый инструментарий и методические указания по выполнению.
3. Критерии оценки результатов выполнения практических работ.\
4. Список рекомендуемой литературы и интернет-ресурсов.

В результате освоения практических занятий по дисциплине «Информационные технологии в профессиональной деятельности» обучающиеся должны **знать:**

– основные нормативные правовые акты в области информационной безопасности и защиты информации, а также нормативные методические документы Федеральной;

– службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю в данной области;

– правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны;

– правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации средств защиты информации;

– организацию ремонтного обслуживания аппаратуры и средств защиты информации;

– принципы и методы организационной защиты информации, организационное обеспечение информационной безопасности в организации;

правовое положение субъектов правоотношений в сфере профессиональной деятельности (включая предпринимательскую деятельность).

уметь:

– осуществлять организационное и правовое обеспечение информационной безопасности телекоммуникационных систем в рамках должностных обязанностей техника по защите информации;

– применять нормативные правовые акты и нормативные методические документы в области защиты информации;

– выявлять каналы утечки информации на объекте защиты;

– контролировать соблюдение персоналом требований режима защиты информации;

– оформлять документацию по регламентации мероприятий и оказанию услуг в области защиты информации;

защищать свои права в соответствии с трудовым законодательством.

Настоящие методические рекомендации призваны обеспечить эффективную организацию и проведение практических занятий по дисциплине ОП.10 «Организационно-правовое обеспечение информационной безопасности», способствовать формированию у обучающихся профессиональной компетентности и успешной адаптации к требованиям современного рынка труда.

Составитель: Белолюбская К.П., преподаватель НПОУ «ЯКИТ»

Список рекомендуемой литературы и источников

Основные источники:

1. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889.

Дополнительные печатные источники:

1. Нетёсова, О. Ю. Информационные технологии в экономике: учебное пособие для среднего профессионального образования / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — Москва: Издательство Юрайт, 2022. — 178 с. — (Профессиональное образование). — ISBN 978-5-534-09107-6. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491753.

2. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497433.

Выполнение и защита практических работ. Практические работы проводятся с целью усвоения и закрепления практических умений и знаний, овладения профессиональными компетенциями.

Список практических работ:

1. Практическая работа № 1 «Классификация нормативно-правовых актов».
2. Практическая работа № 2 «Разработка плана-проекта по внедрению защиты информационной безопасности объекта».
3. Практическая работа № 3 «Юридическая экспертиза входящих документов».
4. Практическая работа № 4 «Разработка методических указаний».
5. Практическая работа № 5 «Работа с персональными данными».

Текущий контроль и оценка результатов обучения учебной дисциплины

ОП.10 Организационно-правовое обеспечение информационной безопасности

Входной контроль по географии

Назначение входного контроля – оценить уровень первичных знаний для выстраивания индивидуальной траектории обучения студентов при получении профессии 40.02.02 Правоохранительная деятельность, по программе базовой подготовки в соответствии с примерной программой учебной дисциплины «Организационно-правовое обеспечение информационной безопасности» для профессий СПО.

На выполнение входного контроля (тестирования)отводится 30 минут.

Инструкция для студентов

1.Форма проведения входного контроля– письменное выполнение работы (тестирование)**.**

2.Принципы отбора содержания текущего контроля ориентация на требования к результатам освоения учебной дисциплины «Организационно-правовое обеспечение информационной безопасности», представленным в рабочей программе учебной дисциплины «Организационно-правовое обеспечение информационной безопасности», пройденным материалом за курс средней школы.

3.Структура входного контроля:

3.1 Входной контроль(тестирование) состоит из 2 равноценных вариантов текстов тестовой работы.

3.2 . Отобранные задания составляют необходимый минимум усвоения знаний и умений в соответствии с требованиями рабочей программы учебной дисциплины «Организационно-правовое обеспечение информационной безопасности» пройденный за курс средней школы.

3.3 . Сдача входного контроля предполагает написание теста по одному варианту.

3.4 . Все варианты тестовой работы равноценны по трудности и одинаковы по структуре.

4.Система оценивания входного контроля (тестирования):

Входной контроль (тестирование): оценивается по 5-тибалльной шкале следующим образом:

оценка «5» (отлично) выставляется за 90-100% правильных ответов;

оценка «4» (хорошо) выставляется за 70-89% правильных ответов;

оценка «3» (удовлетворительно) выставляется за 50-69% правильных ответов;

оценка «2» (неудовлетворительно) выставляется, если количество правильных ответов менее 50%.

Оценка «1»: задание не выполнено.

Соблюдайте последовательность работы:

1.Внимательно прочитайте все вопросы в тестовой работе.

2.Первоначально отвечайте на вопросы, которые являются для вас наиболее посильными.

А затем переходите к ответам н вопросы, которые вызывают затруднения.

Оценочные средства для текущего контроля успеваемости

Раздел 1

Тема 1.3 Виды защищаемой информации

1. Информация, зафиксированная на материальном носителе, с реквизитами, позволяющими ее идентифицировать, называется
· достоверной
· конфиденциальной
· **документированной**
· коммерческой тайной

2. Формы защиты интеллектуальной собственности -
· **авторское, патентное право и коммерческая тайна**
· интеллектуальное право и смежные права
· коммерческая и государственная тайна
· гражданское и административное право

3. По принадлежности информационные ресурсы подразделяются на
· **государственные, коммерческие и личные**
· государственные, не государственные и информацию о гражданах
· информацию юридических и физических лиц
· официальные, гражданские и коммерческие

4. По доступности информация классифицируется на
· открытую информацию и государственную тайну
· конфиденциальную информацию и информацию свободного доступа
· **информацию с ограниченным доступом и общедоступную информацию**
· виды информации, указанные в остальных пунктах

5. К конфиденциальной информации относятся документы, содержащие
· **государственную тайну**
· законодательные акты
· "ноу-хау"
· сведения о золотом запасе страны

6. Конфиденциальная информация это
· сведения, составляющие государственную тайну
· сведения о состоянии здоровья высших должностных лиц
· **документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ**
· данные о состоянии преступности в стране

7. Какая информация подлежит защите?
· информация, циркулирующая в системах и сетях связи
· зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать
· только информация, составляющая государственные информационные ресурсы
· **любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу**

8. Система защиты государственных секретов определяется Законом
· "Об информации, информатизации и защите информации"
· "Об органах ФСБ"
· **"О государственной тайне"**
· "О безопасности"

9. Классификация и виды информационных ресурсов определены
· **Законом "Об информации, информатизации и защите информации"**
· Гражданским кодексом
· Конституцией
· всеми документами, перечисленными в остальных пунктах

10. Формой правовой защиты изобретений является
· институт коммерческой тайны
· **патентное право**
· авторское право
· все, перечисленное в остальных пунктах

Тема 3.1 Международное законодательство в области защиты информации

1. Основные угрозы доступности информации:
- **непреднамеренные ошибки пользователей**
- злонамеренное изменение данных
- хакерская атака
- **отказ программного и аппаратно обеспечения разрушение или повреждение помещений**
- перехват данных

2. Суть компрометации информации
- внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации
- несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений
- **внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений**

3. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …
- **с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды**

− с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации
− способна противостоять только информационным угрозам, как внешним так и внутренним
− способна противостоять только внешним информационным угрозам

4. Методы повышения достоверности входных данных
− **Замена процесса ввода значения процессом выбора значения из предлагаемого множества**
− Отказ от использования данных
− Проведение комплекса регламентных работ
− **Использование вместо ввода значения его считывание с машиночитаемого носителя**
− **Введение избыточности в документ первоисточник**
− Многократный ввод данных и сличение введенных значений

5. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ)
− **МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения**
− МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты
− МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

6. Сервисы безопасности:
− **идентификация и аутентификация шифрование**
− инверсия паролей
− **контроль целостности**
− регулирование конфликтов
− **экранирование**
обеспечение безопасного восстановления
− кэширование записей

7. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …
− **несанкционированного управления удаленным компьютером**
− внедрения агрессивного программного кода в рамках активных объектов Web-страниц
− перехвата или подмены данных на путях транспортировки
− вмешательства в личную жизнь
− поставки неприемлемого содержания

8. Причины возникновения ошибки в данных
− **Погрешность измерений**
− **Ошибка при записи результатов измерений в промежуточный документ**
− Неверная интерпретация данных
− **Ошибки при переносе данных с промежуточного документа в компьютер**
− Использование недопустимых методов анализа данных
− Неустранимые причины природного характера
− **Преднамеренное искажение данных**

− **Ошибки при идентификации объекта или субъекта хозяйственной деятельности**

9. К формам защиты информации не относится…
− **Аналитическая**
− Правовая
− организационно-техническая
− **страховая**

10. Наиболее эффективное средство для защиты от сетевых атак
− **использование сетевых экранов или «firewall»**
− использование антивирусных программ
− посещение только «надёжных» Интернет-узлов
использование только сертифицированных программ-броузеров при доступе к сети Интернет

Критерии оценивания заданий к зачету:

Кол-во баллов	Оценка	Критерии оценки
91 - 100	отлично	студент должен: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; продемонстрировать умения самостоятельной работы с литературой; уметь сделать выводы по излагаемому материалу
71 - 90	хорошо	студент должен: продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; продемонстрировать умение ориентироваться в литературе; уметь сделать достаточно обоснованные выводы по излагаемому материалу
51 - 70	удовлетворительно	студент должен: продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины.
Менее 51	неудовлетворительно	ставится в случае: незнания значительной части программного материала; не владения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу.

2. Промежуточная аттестация по учебной дисциплине ОП.10 Организационно-правовое обеспечение информационной безопасности

Теоретическая часть – тестирование:

1. Государственная тайна - это сведения защищаемые государством в области ..., распространение которых может нанести ущерб безопасности РФ?
A) военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности
B) военной, внешнеполитической, внутриполитической, экономической, научной, разведывательной, контрразведывательной и оперативно-розыскной деятельности
C) военной, экономической, научной, разведывательной, контрразведывательной и оперативно-розыскной деятельности
D) военной, внешнеполитической, внутриполитической, экономической, научной, разведывательной, контрразведывательной деятельности

2. Не реже какого срока, органы государственной власти обязаны пересматривать содержание действующих перечней?
A) 10 лет
B) 5 лет
C) 3 года
D) 6 лет
E) нет верного ответа

3. Кроме исключительных случаев, срок засекречивания сведений, составляющих государственную тайну, не должен превышать?
A) 10 лет
B) 20 лет
C) 25 лет
D) 35 лет
E) нет верного ответа

4. Передача сведений, составляющих государственную тайну, предприятиям, учреждениям, организациям или гражданам осуществляется с разрешения органа государственной власти только при наличии?
A) у предприятия - лицензии, у граждан - допуска
B) у предприятия - сертификата соответствия, у граждан - лицензии
C) у предприятия и граждан - лицензии и сертификата
D) у предприятия - лицензии и сертификата, у граждан - свобода воли при заключении договора
E) нет верного ответа

5. Негосударственные информационные ресурсы принадлежат:
A) Только физическим лицам
B) Только юридическим лицам
C) Оба варианта неверны
D) Оба варианта верны

6. Обладатель информации не вправе:
A) использовать информацию, в том числе распространять ее, по своему усмотрению
B) передавать информацию другим лицам по договору или на ином установленном законом основании

C) оба ответа верны
D) оба ответа неверны

7. Обработка персональных данных может быть осуществлена...
A) А) только с согласия в письменной форме субъекта персональных данных
B) Б) только с согласия в устной форме субъекта персональных данных
C) В) с согласия законного представителя субъекта персональных данных в письменной форме
D) все варианты верны
E) все варианты неверны
F) верны варианты А и Б
G) верны варианты А и В

8. Государственная тайна - это сведения защищаемые государством в области ..., распространение которых может нанести ущерб безопасности РФ?
A) военной, внешнеполитической, внутриполитической, экономической, научной, разведывательной, контрразведывательной и оперативно-розыскной деятельности
B) военной, экономической, научной, разведывательной, контрразведывательной и оперативно-розыскной деятельности
C) военной, внешнеполитической, внутриполитической, экономической, научной, разведывательной, контрразведывательной деятельности
D) военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности

9. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:
A) о степени важности документа
B) об государственном органе либо организации принявшем соответствующий НПА
C) о количестве страниц документа
D) об условиях засекречивания
E) все ответы верны
F) все ответы не верны

10. Информационное законодательство - это?
A) совокупность норм права, регулирующих общественные отношения в информационной сфере
B) совокупность законодательных актов , регулирующих цифровые отношения в информационной сфере
C) совокупность НПА, регулирующих отношения в информационной сфере
D) совокупность правил, устанавливающих отношения в информационной сфере

11. На носители сведений, составляющих государственную тайну, наносятся реквизиты, включающие следующие данные:
A) о степени секретности сведений
B) об государственном органе либо организации осуществивших засекречивание носителя
C) о регистрационном номере
D) о дате рассекречивания
E) об условиях рассекречивания
F) все ответы верны
G) все ответы не верны

Практическая часть:

ЗАДАЧА

Министерство обороны Российской Федерации разработало новый метод обнаружения и глушения беспилотных летательных аппаратов.

Проводимые испытания были зафиксированы на цифровом носителе (смотри картинки 1-3).

Рисунок 1. - Внешний жесткий диск HDD

Интерфейсы и разъемы

Интерфейс	USB 3.0
Вид разъема	Micro USB 3.0; USB 3.0

Накопители данных

Объем накопителя	500 ГБ

Материалы

Материал корпуса	Пластик

Рисунок 2. – Технические характеристики

Рисунок 3. – Внешние параметры

1. Будет ли отнесена данная информация к государственной тайне? Обоснуйте свой ответ.

2. Если считаете, что информация должна быть отнесена к государственной тайне, какой гриф секретности должен быть присвоен данной информации? Обоснуйте свой ответ.

3. Какой документ должен быть подготовлен? Подготовьте этот документ.

Критерии оценивания заданий по экзамену:

Кол-во баллов	Оценка	Критерии оценки
91 - 100	отлично	студент должен: продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; продемонстрировать умения самостоятельной работы с литературой; уметь сделать выводы по излагаемому материалу
71 - 90	хорошо	студент должен: продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; продемонстрировать умение ориентироваться в литературе; уметь сделать достаточно обоснованные выводы по излагаемому материалу
51 - 70	удовлетворительно	студент должен: продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины.
Менее 51	неудовлетворительно	ставится в случае: незнания значительной части программного материала; не владения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу.