МИНОБРНАУКИ РОССИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ФЕДЕРАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ЦЕНТР
«КОЛЬСКИЙ НАУЧНЫЙ ЦЕНТР РОССИЙСКОЙ АКАДЕМИИ НАУК»
(ФИЦ КНЦ РАН)

МЕТОДИЧЕСКИЕ УКАЗАНИЯ К САМОСТОЯТЕЛЬНОЙ РАБОТЕ ОБУЧАЮЩИХСЯ

По дисциплине Б1.В.07 Информационная безопасность организации
указывается цикл (раздел) ОП, к которому относится дисциплина, название дисциплины

для направления подготовки (специальности) 09.04.02 Информационные системы и технологии
код и наименование направления подготовки (специальности)

направленность программы (профиль) Информационные системы предприятий и учреждений
наименование профиля /специализаций/образовательной программы

Квалификация выпускника, уровень подготовки
магистр
(указывается квалификация (степень) выпускника в соответствии с ФГОС ВО)

Апатиты

2020

Лист согласования

1 Разработчик:

доцент УАиМ А.М. Федоров
должность подпись И.О. Фамилия

2 Методические указания рассмотрены и одобрены на заседании учебно-методической комиссии управления аспирантуры и магистратуры 29 июня 2020 г., протокол № 02.

Председатель УМК УАиМ

29.06.2020 Л.Д. Кириллова
дата подпись И.О.Фамилия

Пояснительная записка

1. Методические указания составлены в соответствии с требованиями федерального государственного образовательного стандарта по образовательной программе высшего образования – программе магистратуры по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом Минобрнауки России № 917 от 19.09.2017.

2. **Цель дисциплины (модуля)** «Информационная безопасность организации» – сформировать у обучающихся комплексного представления о современного состояния сферы корпоративной информационной безопасности, в т.ч. в вопросах безопасности информационных систем и обрабатываемых в них персональных данных.

Задачи дисциплины:

- развить представление о современных проблемах информационной безопасности;
- научиться критически анализировать ситуации, связанные с защитой информации;
- получить представление способах организации и обеспечения информационной безопасности на предприятии.

3. **Требования к уровню подготовки обучающегося** в рамках данной дисциплины.

Процесс изучения дисциплины (модуля) «Информационная безопасность организации» направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО 09.04.02 Информационные системы и технологии (уровень магистратуры), представленных в таблице 1.

Таблица 1 – Компетенции, формируемые в процессе изучения дисциплины «Информационная безопасность организации»

№ п/п	Код компетенции	Содержание компетенции
1.	ПК - 5	Способен анализировать и строить оценки и прогнозы в отношении процессов и объектов в профессиональной научной деятельности

4. Планируемые результаты обучения по дисциплине (модулю) «Информационная безопасность организации».

Результаты формирования компетенций и обучения представлены в таблице 2.

Таблица 2 – Планируемые результаты обучения

№ п/п	Код компетенции	Компоненты компетенции, степень их реализации	Результаты обучения
1.	ПК - 5	Компоненты компетенции соотносятся с содержанием дисциплины и компетенция реализуется полностью	***Знать:*** основные стандарты, средства и методы применения информационных систем и технологий в различных областях профессиональной деятельности (ПК -

			5.1). ***Уметь:*** с помощью информационных технологий проводить анализ, оценку и прогноз при решении задач в различных областях профессиональной деятельности (ПК -5.2). ***Владеть:*** навыками планирования, организации у управления процессами решения задач с помощью подходящих информационных технологий и систем в различных областях профессиональной деятельности (ПК- 5.3).

ПЕРЕЧЕНЬ РЕКОМЕНДУЕМОЙ ЛИТЕРАТУРЫ

Основная:

1. Галатенко, В.А. Основы информационной безопасности: Курс лекций / В.А. Галатенко ; под ред. В.Б. Бетелина. – Изд. 3-е. – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2006. – 208 с. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=233063 (дата обращения: 02.12.2020). – ISBN 5-9556-0052-3. – Текст : электронный.
2. Ищейнов, В.Я. Информационная безопасность и защита информации: теория и практика : учебное пособие : [16+] / В.Я. Ищейнов. – Москва ; Берлин : Директ-Медиа, 2020. – 271 с. : схем., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=571485 (дата обращения: 02.12.2020). – Библиогр. в кн. – ISBN 978-5-4499-0496-6. – DOI 10.23681/571485. – Текст : электронный.
3. Гультяева, Т.А. Основы защиты информации : учебное пособие : [16+] / Т.А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2018. – 83 с. : ил., табл. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=574730 (дата обращения: 15.12.2020). – Библиогр. в кн. – ISBN 978-5-7782-3641-7. – Текст : электронный.

Дополнительная:

4. Философские проблемы информационного противоборства: учебное пособие для бакалавров, студентов, магистрантов и аспирантов / В.С. Поликарпов, В.Е. Шибанов, Е.В. Поликарпова, К.Е. Румянцев ; Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2018. – 211 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=499981 (дата обращения: 02.12.2020). – Библиогр. в кн. – ISBN 978-5-9275-2716-8. – Текст : электронный.
5. Пелешенко, В.С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления : учебное пособие / В.С. Пелешенко, С.В. Говорова, М.А. Лапина ; Северо-Кавказский федеральный университет. – Став-

рополь : Северо-Кавказский Федеральный университет (СКФУ), 2017. – 86 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=467139 (дата обращения: 02.12.2020). – Библиогр. в кн. – Текст : электронный.

6. Смолина, В.А. SMM С НУЛЯ: секреты продвижения в социальных сетях / В.А. Смолина. – Москва ; Вологда : Инфра-Инженерия, 2019. – 353 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=564678 (дата обращения: 15.12.2020). – ISBN 978-5-9729-0259-0. – Текст : электронный.
7. Шелудько, В.М. Основы программирования на языке высокого уровня Python : учебное пособие / В.М. Шелудько ; Министерство науки и высшего образования РФ, Южный федеральный университет, Инженерно-технологическая академия. – Ростов-на-Дону ; Таганрог : Южный федеральный университет, 2017. – 147 с. : ил. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=500056 (дата обращения: 15.12.2020). – Библиогр. в кн. – ISBN 978-5-9275-2649-9. – Текст : электронный.
8. Защита персональных данных в информационных системах: лабораторный практикум / авт.-сост. В.И. Петренко, И.В. Мандрица ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2018. – 118 с. – Режим доступа: по подписке. – URL: https://biblioclub.ru/index.php?page=book&id=494823 (дата обращения: 15.12.2020). – Текст : электронный.

СОДЕРЖАНИЕ ПРОГРАММЫ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

1. Понятие Информационной безопасности. Специфика решений задач информационной безопасности для различных типов предприятий и организаций. Объектно-ориентированный подход для решения задач информационной безопасности.

Вопросы для самоконтроля знаний:

1. Информационная безопасность
2. Безопасность информации
3. Защита информации- ментальная карта понятий - тезисы
4. Что такое информационная безопасность?
2. Что является основными составляющими информационной безопасности?
3. Какие цели и задачи имеет информационная безопасность?
4. В чем заключается важность и сложность проблемы информационной безопасности?

Рекомендуемая литература: [1], [2], [3], [7]

2. Классификации угроз информационной безопасности. Корпоративная и персональная "информационная гигиена", "информационные ОБЖ", управление рисками ИБ.

Вопросы для самоконтроля знаний:

1. Основные определения и критерии классификации угроз [];
2. Наиболее распространенные угрозы доступности [];
3. Примеры угроз доступности;
4. Программные атаки на доступность;
5. Вредоносное программное обеспечение;
6. . Основные угрозы целостности [];
7. . Основные угрозы конфиденциальности [];

Рекомендуемая литература: [1], [2], [3], [7]

3. Обзор актуальной новостной повестки по теме информационная безопасность на уровнях: государство, крупные корпорации, средний и малый бизнес, профильные сектора экономики и т.п.

Вопросы для самоконтроля знаний:

1. Порталы корпоративной новостной информации со спецификой информационной безопасности
2. Протоколирование и аудит
3. Активный аудит
4. Шифрование
5. Контроль целостности
6. Для чего предназначена и какую роль в ИБ играет сервис:
7. Как и с какими угрозами ИБ позволяет бороться сервис:
    a. Экранирование;
    b. Анализ защищенности.

Рекомендуемая литература: [1], [2], [3], [7]

4. Законодательный уровень информационной безопасности. Доктрина информационной безопасности РФ. Персональные данные. Интеллектуальная собственность, авторские права, служебное произведение, лицензирование.

Вопросы для самоконтроля знаний:

1. Что такое законодательный уровень информационной безопасности и почему он важен []
2. Обзор российского законодательства в области информационной безопасности
3. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности []
4. Другие законы и нормативные акты РФ
5. Обзор зарубежного законодательства в области информационной безопасности
6. О текущем состоянии российского законодательства в области информационной безопасности
7.

Рекомендуемая литература: [1], [2]

5. Административный и процедурный уровни информационной безопасности для предприятий и организаций. Корпоративная политика использования внешних коммуникаций: персональные мобильные устройства, социальные сети, мессанджеры и др. сервисы.

Вопросы для самоконтроля знаний:

1. Административный уровень информационной безопасности:
2. Основные понятия []
3. Политика безопасности []
4. Программа безопасности
5. Синхронизация программы безопасности с жизненным циклом систем.
6. В чем заключается и для чего предназначен "процедурный уровень информационной безопасности"?
7. . Каковы цели и особенности реализации указанного класса мер процедурного уровня ИБ?
8. . Управление персоналом
9. . Физическая защита
10. . Поддержание работоспособности
11. . Реагирование на нарушения режима безопасности
12. Планирование восстановительных работ

Рекомендуемая литература: [1], [2], [3], [7].

6. Классификация программно-технических средств обеспечения информационной безопасности: идентификация и аутентификация; управление доступом, протоколирование, аудит, шифрование, электронная цифровая подпись, антивирусная защита.

Вопросы для самоконтроля знаний:

1. В чем заключается и для чего предназначен "программно-технический уровень информационной безопасности"?

2. Почему средства по обеспечению безопасности в информационных системах называются "сервисами"? Что такое "полный набор сервисов ИБ" и как можно классифицировать сервисы в нем?
3. Какие особенности современных информационных систем являются существенными с точки зрения организации информационной безопасности на программно-техническом уровне?
4. Что означает и какое место в обеспечении информационной безопасности занимает архитектурная безопасность?
5. Для чего предназначена и какую роль в ИБ играет сервис X?
6. Какие существуют способы реализации сервиса X и в чем их особенности?
7. . пара сервисов "идентификация" и "аутентификация";
8. . сервис "управление доступом".
9. Управление ролями пользователей в корпоративных информационных системах. Основные принципы администрирования
10. Антивирусная защита компьютерных систем
11. Вирусы и средства борьбы с ними
12. Основы информационной безопасности при работе на компьютере
13. Инфраструктуры открытых ключей

Рекомендуемая литература: [1], [2].

7. Открытые данные информационного пространства и угрозы корпоративной безопасности. Юридические и этические вопросы извлечения и анализа открытых данных социальных сетей. Программные средства анализа социальных сетей. Практические задачи анализа открытых данных социальных сетей.

Вопросы для самоконтроля знаний:
1. Для чего предназначена и какую роль в ИБ играет сервис X?
2. Какие существуют способы реализации сервиса X и в чем их особенности?
3. Почему пара сервисов X обычно рассматривается совместно друг с другом?
4. . пара сервисов "протоколирование" и "аудит";
5. . пара сервисов "шифрование" и "контроль целостности".
6. Что такое, как реализуется и где используется "электронная цифровая подпись"?.

Рекомендуемая литература: [1], [2], [3].

8. Решение задач информационной безопасности при проектировании и разработке информационных систем и программных приложений. Использование сторонних сервисов информационной безопасности

Вопросы для самоконтроля знаний:
1. Базовые понятия и Терминология
2. Криптографические примитивы
3. . Криптографические хэш-функции
4. Криптографические генераторы псевдослучайных чисел
5. Модели основных криптоаналитических атак
6. Анализ стойкости криптографических примитивов
7. Практические рекомендации по использованию шифрования
8. Криптографическое преобразование информации: методы подстановки.
9. = Моноалфавитные подстановки. Шифр Цезаря
10. Многоалфавитные подстановки. Шифр Вижинера

11. Монофонические шифры
12. Частотный анализ.

Рекомендуемая литература: [1], [2], [3].

КОНТРОЛЬНЫЕ ВОПРОСЫ

Итоговый уровень знаний обучающихся, приобретенный при изучении дисциплины «Информационная безопасность организации», проверяется на экзамене.

Для проверки теоретической подготовки студентов по дисциплине, на экзамен выносятся следующие вопросы:

1. Понятие информационной безопасности. Основные составляющие информационной безопасности.
2. Важность и сложность проблемы информационной безопасности
3. Законодательный уровень информационной безопасности. Российское законодательство в области информационной безопасности
4. Объектно-ориентированный подход к информационной безопасности: основные понятия, достоинства применения
5. Основные определения и критерии классификации угроз
6. Угрозы доступности. Основные угрозы целостности. Угрозы конфиденциальности.
7. Административный уровень информационной безопасности. Политика безопасности информационных систем.
8. Процедурный уровень информационной безопасности: классы мер и принципы их реализации.
9. Программно-технические меры безопасности. Понятие сервиса информационной безопасности. Архитектурная безопасность.
10. Понятие сервиса информационной безопасности. Идентификация и аутентификация. 11. Понятие сервиса информационной безопасности. Управление доступом.
12. Понятие сервиса информационной безопасности. протоколирование и аудит.
13. Понятие сервиса информационной безопасности. управление и анализ защищенности.
14. Понятие сервиса информационной безопасности. обеспечение высокой доступности и отказоустойчивости.
15. Понятие сервиса информационной безопасности. экранирование и туннелирование.
16. Понятие сервиса информационной безопасности. криптография: шифрование.
17. Понятие сервиса информационной безопасности. криптография: контроль целостности.
18. Криптология: базовые понятия и терминология.
19. Криптографические примитивы и их свойства.
20. Модели основных криптоаналитических атак.
21. Антивирусная защита. История развития вирусов и их классификация. Методы защиты от вредоносных программ

Рекомендуемая литература: [1], [2], [3], [4], [5], [6], [7], [8].