**МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**
**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**
**«Национальный исследовательский Нижегородский государственный университет им. Н.И. Лобачевского»**

Институт экономики и предпринимательства
Кафедра информационных технологий и инструментальных методов в экономике

СОГЛАСОВАНО
Ученым Советом ННГУ
30 ноября 2022 г.
протокол № 13

# Рабочая программа дисциплины
# «Защита информации»

Уровень высшего образования

Магистратура

Направление подготовки

09.04.03 "Прикладная информатика»

Направленность образовательной программы
Интернет-технологии в экономике

Форма обучения
очная, заочная

Нижний Новгород
2023

**1. Место и цели дисциплины в структуре ООП**

Дисциплина Б1.В.ДВ.01.01 «Защита информации» относится к части, формируемой участниками образовательных отношений. Изучается студентами в 3 семестре на 2 курсе.

**2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)**

| **Формируемые компетенции** (код, содержание компетенции) | **Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции** | | **Наименование оценочного средства** |
|---|---|---|---|
| | **Индикатор достижения компетенции*** (код, содержание индикатора) | **Результаты обучения по дисциплине**** | |
| *ПК-4* Способен формировать гибкую стратегию информатизации прикладных процессов на основе интеллектуальных информационных систем (ИИС), адаптирующихся к стратегии развития предприятий | *ПК-4.1* *Знать:* основные задачи и понятия кодирования, методы и средства защиты информации; *ПК-4.2.* *Уметь:* применять современный инструментарий теории защиты информации: нормативные документы по информационной безопасности. *ПК-4.3.* *Владеть:* навыками применения современного инструментария кодирования и защиты информации. | *Знать:*<br>• основные задачи и понятия кодирования, методы и средства защиты информации;<br>*Уметь:*<br>• применять современный инструментарий теории защиты информации.<br>• нормативные документы по информационной безопасности.<br>*Владеть:* навыками применения современного инструментария защиты информации. | Тесты, доклады, практические задания |

| | | | |
|---|---|---|---|
| *ПК-8* Способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств | *ПК-8.1.* *Знать:* особенности сервиса, связанного с защитой информации *ПК-8.2.* *Уметь:* встраивать процедуры защиты информации в архитектуру ИС. *ПК-8.3.* *Владеть:* методами оценки эффективности инвестиций в информационной безопасности. | *Знать:* особенности сервиса, связанного с защитой информации *Уметь:* встраивать процедуры защиты информации в архитектуру ИИС. *Владеть:* методами оценки эффективности инвестиций в информационной безопасности. | Тесты, доклады, практические задания |
| *ПК-9.* Способен руководить проектами по созданию и модернизации гибридных ИИС, базирующихся на концепции системы, основанной на знаниях, и современных нейросетевых технологиях принятия решений. | ПК-9.1. Способен использовать базовые принципы концепции системы, основанной на знаниях, и нейросетевой парадигмы принятия решений при планировании проектов гибридных ИИС ПК-9.2. Способен организовать командный подход к созданию и модернизации гибридных ИИС.Способен руководить конкретными проектами по созданию и модернизации гибридных ИИС. | *ПК-9.1* *Знать:* особенности защиты информации при проектировании гибридных ИИС; *Уметь:* встраивать процедуры защиты информации в архитектуру гибридных ИИС. *Владеть:* методами оценки эффективности защиты информации в гибридных ИИС. ПК-9.2 *Знать:* особенности организации системы защиты информации при проектировании гибридных ИИС; *Уметь:* организовать систему защиты информации в гибридной ИИС. *Владеть:* навыками командной работы при организации системы защиты информации гибридных ИИС. | Тесты, доклады, практические задания |

## 3. Структура и содержание дисциплины

### 3.1. Трудоемкость дисциплины

| | очная форма обучения | заочная форма обучения |
|---|---|---|
| **Общая трудоемкость** | **6 ЗЕТ** | **6 ЗЕТ** |
| **Часов по учебному плану** | **216** | **216** |
| **в том числе** | | |
| **аудиторные занятия (контактная работа):**<br>**- занятия лекционного типа**<br>**- занятия семинарского типа**<br>**- текущий контроль** | **34**<br>**6**<br>**26**<br>**2** | **20**<br>**4**<br>**14**<br>**2** |
| **самостоятельная работа** | **128** | **187** |
| **Промежуточная аттестация – экзамен** | **экзамен** | **экзамен** |

## 3.2. Содержание дисциплины

| Наименование и краткое содержание разделов и тем дисциплины | Всего | | | в том числе | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Контактная работа (работа во взаимодействии с преподавателем), часы из них | | | | | | | | | | | Самостоятельная работа обучающегося, часы | | |
| | | | | Занятия лекционного типа | | | Занятия семинарского типа | | | Занятия лабораторного типа | | Всего | | | | | |
| | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Очная | Очно-заочная | Заочная | Очная | Очно-заочная | Заочная |
| Тема 1. Теоретические аспекты системы защиты информации | 28 | | 32 | 1 | | | 4 | | | | | 5 | | 0 | 23 | | 32 |
| Тема 2. Понятие информационных угроз и их виды | 26 | | 33 | 1 | | | 4 | | 2 | | | 5 | | 2 | 21 | | 31 |
| Тема 3. Государственное регулирование защиты информации | 26 | | 34 | 1 | | 1 | 4 | | 2 | | | 5 | | 3 | 21 | | 31 |
| Тема 4. Подходы, принципы, методы и средства защиты информации | 26 | | 36 | 1 | | 1 | 4 | | 4 | | | 5 | | 5 | 21 | | 31 |
| Тема 5. Криптографические средства защиты информации | 26 | | 36 | 1 | | 1 | 4 | | 4 | | | 5 | | 5 | 21 | | 31 |
| Тема 6. Организация системы защиты информации | 28 | | 34 | 1 | | 1 | 6 | | 2 | | | 7 | | 3 | 21 | | 31 |
| В т.ч. текущий контроль | | | | | | | 2 | | 2 | | | | | | | | |
| Итого | 216 | | 216 | 6 | | 4 | 28 | | 16 | | | 34 | | 20 | 128 | | 187 |

Практические занятия организуются, в том числе в форме **практической подготовки**, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

**Практическая подготовка** предусматривает решение прикладной практической задачи, связанной с применением современных инструментов менеджмента для организации процесса менеджмента рисков информационной безопасности на предприятии и организации системы защиты информации.

На проведение практических занятий в форме практической подготовки отводится 6 часов.

**Практическая подготовка** направлена на формирование и развитие:

- практических навыков в соответствии с профилем ООП (навыков решения типовых задач профессиональной деятельности **научно-исследовательского типа** (исследование прикладных и информационных процессов, использование и разработка методов формализации информационных процессов; анализ и обобщение результатов научно-исследовательской работы с использованием современных достижений науки и техники; анализ и развитие методов управления информационными ресурсами); **организационно-управленческого типа** (организация и управление информационными процессами; организация и управление проектами по информатизации предприятий; организация ИС в прикладной области; управление ИС и сервисами; управление персоналом ИС; разработка учебных программ переподготовки персонала ИС и проведение обучения пользователей; принятие решений по организации внедрения ИС на предприятиях; организация и проведение профессиональных консультаций в области информатизации предприятий и организаций; организация и проведение переговоров с представителями заказчика; организация работ по сопровождению и эксплуатации прикладных ИС); **проектного типа** (определение стратегии использования ИКТ для создания ИС в прикладных областях, согласованной со стратегией развития организации; проведение реинжиниринга прикладных информационных и бизнес процессов; проведение технико-экономического обоснования проектных решений и разработка проектов информатизации предприятий и организаций в прикладной области в соответствии с профилем; адаптация и развитие прикладных ИС на всех стадиях жизненного цикла));
- компетенций (*ПК-4* Способен формировать гибкую стратегию информатизации прикладных процессов на основе интеллектуальных информационных систем (ИИС), адаптирующихся к стратегии развития предприятий; *ПК-8* Способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств; *ПК-9.* Способен руководить проектами по созданию и модернизации гибридных ИИС, базирующихся на концепции системы, основанной на знаниях, и современных нейросетевых технологиях принятия решений).

**Текущий контроль** успеваемости реализуется в рамках практических занятий.

**Промежуточная аттестация** проходит в традиционных форма (зачет, экзамен), в иных формах (бально-рейтинговая система, комплексный экзамен, включающий выполнение практических заданий (возможно наряду с традиционными ответами на вопросы по программе дисциплины)).

## 4. Учебно-методическое обеспечение самостоятельной работы обучающихся

Цель самостоятельной работы - формирование навыков непрерывного самообразования и профессионального совершенствования.

Самостоятельная работа способствует формированию аналитического и творческого мышления, совершенствует способы организации исследовательской деятельности, воспитывает целеустремленность, системность и последовательность в работе студентов, развивает у них навык завершать начатую работу.

**Основные виды самостоятельной работы студентов**:

- работа с основной и дополнительной литературой;
- изучение категориального аппарата дисциплины;
- самостоятельное изучение тем дисциплины;
- подготовка докладов-презентаций;
- подготовка к экзамену;
- работа в библиотеке;
- изучение сайтов по темам дисциплины в сети Интернет.

**Работа с основной и дополнительной литературой**

Изучение рекомендованной литературы следует начинать с учебников и учебных пособий, затем переходить к научным монографиям и материалам периодических изданий. Работа с литературой предусматривает конспектирование наиболее актуальных и познавательных материалов. Это не только мобилизует внимание, но и способствует более глубокому осмыслению материала, его лучшему запоминанию, а также позволяет студентам проводить систематизацию и сравнительный анализ изучаемой информации. Таким образом, конспектирование – одна из основных форм самостоятельного труда, которая требует от студента активно работать с учебной литературой и не ограничиваться конспектом лекций.

Студент должен уметь самостоятельно подбирать необходимую литературу для учебной и научной работы, уметь обращаться с предметными каталогами и библиографическим справочником библиотеки.

**Изучение категориального аппарата дисциплины**

Изучение и осмысление категорий дисциплины требует проработки лекционного материала, выполнения практических заданий, изучение словарей, энциклопедий, справочников.

Индивидуальная самостоятельная работа студента направлена на овладение и грамотное применение терминологии в области изучаемой дисциплины.

**Самостоятельное изучение тем дисциплины**

Особое место отводится самостоятельной проработке студентами отдельных разделов и тем изучаемой дисциплины. Такой подход вырабатывает у студентов инициативу, стремление к увеличению объема знаний, умений и навыков, всестороннего овладения способами и приемами профессиональной деятельности.

Изучение вопросов определенной темы направлено на более глубокое усвоение основных категорий теории, понимание изучаемых процессов, совершенствование навыка анализа теоретического и эмпирического материала.

**Подготовка докладов-презентаций**

Написание докладов и подготовка презентации позволяет студентам глубже изучить темы курса, самостоятельно освоить изучаемый материал, пользуясь учебными пособиями и научными работами. Тема доклада может назначаться преподавателем или инициироваться студентом.

**Подготовка к экзамену**

Промежуточная аттестация студентов по дисциплине проходит в виде экзамена и предусматривает оценку. Условием успешного прохождения промежуточной аттестации является систематическая работа студента в течение семестра. В этом случае подготовка к экзамену является систематизацией всех полученных знаний по данной дисциплине.

Рекомендуется внимательно изучить перечень вопросов к экзамену, а также использовать в процессе обучения программу, материалы электронного курса, другие рекомендованные материалы.

Желательно спланировать троекратный просмотр материала перед экзаменом. Во-первых, внимательное чтение с осмыслением, подчеркиванием и составлением краткого плана ответа. Во-вторых, повторная проработка наиболее сложных вопросов. В-третьих, быстрый просмотр материала или планов ответов для его систематизации в памяти.

**Самостоятельная работа в библиотеке**

Важным аспектом самостоятельной подготовки студентов является работа с библиотечным фондом.

Это работа предполагает различные варианты повышения профессионального уровня студентов:

а) получение книг для подробного изучения в течение семестра на научном абонементе;

б) изучение книг, журналов, газет - в читальном зале;

в) возможность поиска необходимого материала посредством электронного каталога;

г) получение необходимых сведений об источниках информации у сотрудников библиотеки.

**Изучение сайтов по темам дисциплины в сети Интернет**

Ресурсы Интернет являются одним из альтернативных источников быстрого поиска требуемой информации. Их использование возможно для получения основных и дополнительных сведений по изучаемым материалам. Необходимо помнить об оформлении ссылок на Интернет-источники.

Для повышения эффективности самостоятельной работы студентов преподавателю целесообразно использовать следующие виды деятельности:

- консультации,
- выдача заданий на самостоятельную работу,
- информационное обеспечение обучения,
- контроль качества самостоятельной работы студентов.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

Для обеспечения самостоятельной работы обучающихся используется электронный курс «Защита информации», расположенный https://e-learning.unn.ru/course/view.php?id=4406 в системе электронного обучения ННГУ - https://e-learning.unn.ru/.

**5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю)**, включающий:

**5.1. Описание шкал оценивания результатов обучения по дисциплине**

| **Уровень сформированности компетенций (индикатора достижения компетенций)** | **Шкала оценивания сформированности компетенций** | | | | | | |
|---|---|---|---|---|---|---|---|
| | **плохо** | **неудовлетворительно** | **удовлетворительно** | **хорошо** | **очень хорошо** | **отлично** | **превосходно** |
| | **не зачтено** | | **зачтено** | | | | |
| Знания | Отсутствие знаний теоретического материала.<br><br>Невозможность оценить полноту знаний вследствие отказа обучающегося от ответа | Уровень знаний ниже минимальных требований. Имели место грубые ошибки. | Минимально допустимый уровень знаний. Допущено много негрубых ошибки. | Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых ошибок | Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественных ошибок | Уровень знаний в объеме, соответствующем программе подготовки, без ошибок. | Уровень знаний в объеме, превышающем программу подготовки. |
| Умения | Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа | При решении стандартных задач не продемонстрированы основные умения.<br><br>Имели место грубые ошибки. | Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме. | Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами. | Продемонстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами. | Продемонстрированы все основные умения,реше-ны все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме. | Продемонстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном<br><br>объеме без недочетов |
| Навыки | Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа | При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки. | Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами | Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами | Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов. | Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов. | Продемонстрирован творческий подход к решению нестандартных задач |

**Шкала оценки при промежуточной аттестации**

| Оценка | | Уровень подготовки |
|---|---|---|
| | **превосходно** | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой |
| **зачтено** | **отлично** | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично» |
| | **очень хорошо** | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо» |
| | **хорошо** | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо» |
| | **удовлетворительно** | Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция сформирована на уровне «удовлетворительно» |
| **не зачтено** | **неудовлетворительно** | Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо» |
| | **плохо** | Хотя бы одна компетенция сформирована на уровне «плохо» |

**5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения**.

**5.2.1 Контрольные вопросы к экзамену**

| *Вопрос* | *Код компетенции* |
|---|---|
| 1. Прогресс информационных технологий и необходимость обеспечения информационной защиты информации. | *ПК-4* |
| 2. Основные понятия теории кодирования и защиты информации. | *ПК-4* |
| 3. Система защиты информации и ее структура. | *ПК-4* |
| 4. Экономическая информация как товар и объект безопасности. | *ПК-4* |
| 5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии. | *ПК-4* |
| 6. Персональные данные и их защита. | *ПК-4* |
| 7. Информационные угрозы, их виды и причины возникновения. | *ПК-4* |
| 8. Информационные угрозы для государства. | *ПК-4* |

| | |
|---|---|
| 9. Информационные угрозы для компании. | *ПК-4* |
| 10. Информационные угрозы для личности (физического лица). | *ПК-4* |
| 11. Действия и события, нарушающие систему защиту информации. | *ПК-4* |
| 12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз. | *ПК-4* |
| 13. Способы воздействия информационных угроз на объекты. | *ПК-4* |
| 14. Внешние и внутренние субъекты информационных угроз. | *ПК-4* |
| 15. Компьютерные преступления и их классификация. | *ПК-4* |
| 16. Исторические аспекты компьютерных преступлений и современность. | *ПК-4* |
| 17. Субъекты и причины совершения компьютерных преступлений. | *ПК-4* |
| 18. Вредоносные программы, их виды. | *ПК-8* |
| 19. История компьютерных вирусов и современность. | *ПК-8* |
| 20. Государственное регулирование информационной безопасности. | *ПК-4* |
| 21. Деятельность международных организаций в сфере информационной безопасности. | *ПК-4* |
| 22. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации. | *ПК-4* |
| 23. Доктрина информационной безопасности России. | *ПК-4* |
| 24. Уголовно-правовой контроль над компьютерной преступностью в России. | *ПК-4* |
| 25. Федеральные законы по ИБ в РФ. | *ПК-4* |
| 26. Политика безопасности и ее принципы. | *ПК-8* |
| 27. Фрагментарный и системный подход к защите информации. | *ПК-8* |
| 28. Методы и средства защиты информации. | *ПК-8* |
| 29. Организационное обеспечение защиты информации | *ПК-8* |
| 30. Организация конфиденциального делопроизводства. | *ПК-8* |
| 31. Комплекс организационно-технических мероприятий по обеспечению защиты информации. | *ПК-8* |
| 32. Инженерно-техническое обеспечение компьютерной безопасности. | *ПК-9* |
| 33. Организационно-правовой статус службы безопасности. | *ПК-8* |
| 34. Защита информации в Интернете. | *ПК-9* |
| 35. Электронная почта и ее защита. | *ПК-9* |
| 36. Защита от компьютерных вирусов. | *ПК-8* |
| 37. «Больные» мобильники и их «лечение». | *ПК-8* |
| 38. Популярные антивирусные программы и их классификация. | *ПК-8* |
| 39. Организация системы защиты информации экономических объектов. | *ПК-8* |
| 40. Теория кодирования и криптографические методы защиты информации. | *ПК-9* |
| 41. Этапы построения системы защиты информации. | *ПК-8* |
| 42. Оценка эффективности инвестиций в информационную безопасность. | *ПК-8* |
| 43. План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы. | *ПК-8* |
| 44. Менеджмент и аудит защиты информации на уровне предприятия. | *ПК-8* |
| 45. Информационная безопасность предпринимательской деятельности. | *ПК-8* |
| 46. Обеспечение защиты информации должностных лиц и представителей деловых кругов. | *ПК-8* |

| | |
|---|---|
| 47. Симметричные и асимметричные системы шифрования. | *ПК-9* |
| 48. Управление рисками защиты информации. | *ПК-8* |
| 49. Аудит кодирования и защиты информации. | *ПК-8* |
| 50. Защита информации в каналах связи сети Интернет. | *ПК-9* |

### 5.2.2. Типовые тестовые задания для оценки результатов обучения, характеризующих этапы формирования компетенций

**Тестовые задания**

*На каждый вопрос предложено три варианта ответа. Выберите один правильный и отметьте его √*

**Тест для оценки компетенции ПК-4:**

1. Правовое обеспечение информационной безопасности - это?
- нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
- документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
- широкое использование технических средств защиты информации.

2. Первым этапом построения системы защиты является:
- анализ;
- планирование;
- сопровождение.

3. «Троянский конь»- это …?
- способ, состоящий в тайном введении в чужую программу вредоносных команд;
- встраивание в программу набора команд, срабатываемых при определенных условиях;
- проникновение в компьютерную систему злоумышленников, выдающих себя за законного пользователя.

4. В политике безопасности основным принципом является усиление самого слабого звена?
- нет;
- да;
- отчасти.

5. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети предусмотрено в ..?
- ст. 272 УК РФ;
- ст. 273 УК РФ;
- ст. 274 УК РФ.

**Тест для оценки компетенции «ПК-9»:**

1. Шифрование с симметричным ключом предполагает, что..?
- используются два разных ключа;
- оба ключа одинаковы;
- невозможно отказаться от авторства.

2. Криптографические средства - это..?
- регламентация правил использования, обработки и передачи информации ограниченного доступа;
- средства защиты с помощью преобразования информации (шифрование);
- средства, в которых программные и аппаратные части полностью взаимосвязаны.

3. Нужно ли предусматривать процедуры защиты информации, если в данное время компьютер не работает в сети?
- нет;
- да;
- да, при подключении к сети.

4. Нужно ли предусматривать процедуры защиты информации, если никогда компьютер не работает в сети?
- нет;
- да;
- да, поскольку используются переносные носители информации.

5. Нужно ли предусматривать процедуры защиты информации, если никогда компьютер не работает в сети и не используются переносные носители?
- нет;
- да;
- да, поскольку возможно подключение к компьютеру.

6. Какой метод использован для шифрования?
Исходное задание -

Гамма: безопасность

нгмшпйъппфьзкчдосьсэбсвкнфкшюьс*саьсбуняайраэадожпзфбмынрмтаричсясыъшгоьрерэршчьшытннфк

Ответ-

Гамма: безопасность

люди избавились бы от половины своих неприятностей если бы договорились о значении слов

- блочный шифр;
- гаммирование;
- перестановка с ключевым словом.

7. Какой метод использован для шифрования?
Исходное задание -

Ключ: наука

апаабеазвыояинмт*аое*лаииеемяочсмастцао*вь*тмюере*пааз*тыепдси*авзбхт*ахдкмт*рсаол*плх*гноьсндсеонозтииысивиайн*гн*бфи*бгонооемдсвйарлтчниу*о*евр*иуоемо*нм*х*вяао*стбни*вв*г*с*шни*ркри

Ответ-

Наука помогает нам в борьбе с фанатизмом в любых его проявлениях она помогает нам создать собственный идеал справедливости ничего не заимствуя из ошибочных систем и варварских традиций

- блочный шифр;
- гаммирование;
- перестановка с ключевым словом.

8. Какой метод использован для шифрования?
Исходное задание -

Ключ (2;4) Шифротекст: ФЗТЫ

Ответ - Соль

- блочный шифр;
- гаммирование;
- перестановка с ключевым словом.

**Для оценки компетенции ПК-8**

1. Третьим этапом построения системы защиты является:

- планирование;

- реализация;
- анализ.

2. «Люком» называется?
- использование после окончания работы части данных, оставшиеся в памяти;
- передача сообщений в сети от имени другого пользователя;
- неописанная в документации на программный продукт возможность работы с ним.

3. К активным угрозам относятся:
- попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания;
- разрушение или радиоэлектронное подавление линий связи, вывод из строя ПЭВМ или ее операционной системы;
- копирование информации.

4. Какого подхода к обеспечению безопасности информации не существует?
- комплексный;
- фрагментарный;
- теоретический.

5. Типовыми путями несанкционированного доступа к информации, являются:
- дистанционное фотографирование;
- выход из строя ПЭВМ;
- ураганы.

### 5.2.3. Типовые практические задания для оценки сформированности компетенции

**ПК-4**

1. Изучить ГОСТ Р 50922-2006. В файле изложить определения защиты информации, угрозы безопасности информации, уязвимости информационной системы и выслать его преподавателю на проверку в системе ЭК.
2. Изучить ГОСТ Р 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент рисков информационной безопасности». Выбрать по 3 угрозы безопасности из списка возможных угроз и изложить в файле мероприятия по противодействию выбранным угрозам, подразделяя их на группы (правовые, организационные, технические). Файл выслать на проверку преподавателю в системе ЭК. ГОСТ прилагается в задании.

**ПК-9**

1. Дешифровать шифротекст, используя алгоритм перестановки с ключевым словом. Полученный исходный текст направить в файле на проверку преподавателю в системе ЭК.

Вариант 104
Ключ: АБСТРАКЦИЯ
НККПРКАО*ЭЗС**ГЫБЕВОАОЛ*Э*ИОЕЙМЕВВАСЬОЕОЕААЛОАЗ*ЗМЫТВИО*ИТЕЛЙИОХ***ТЯВОЕИН*СИС*КРОИТМС*Н**ГАОДП*Ж*МТГПО*АЛГЧИЕТИИТИСБОНТТКОШЗВТНОВРЫ**ПЛЬНЕ*Е*ХОКИОАЦААЖЖСРИ*НЗОИХ*ОЫЬЧИССИНТАОВЕВ***ОСРДО*Я*ЙЯОМОДТП

2. Дешифровать шифротекст, используя алгоритм гаммирования. Полученный исходный текст направить в файле на проверку преподавателю в системе ЭК.

Вариант 101

Гамма - МЕНЕДЖМЕНТ

ШФСЙЕЖДКЪБПКЩЕЦЯНЧАЯЦЗНФТЖПЧУЦСЁНЫУШЬЮНАЬЕЬКДЙЯКСЧНЕГФХЦЕОУТЩГТОДИЗЗОР*Е*ЭЕЩ*СЧХЗ

**ПК-8**

1. Разработать программное обеспечение, реализующее один алгоритм шифрования и позволяющее шифровать сообщения длиной до 150 символов, а также дешифровать их с использованием ключа. Файл с программным кодом приложить как ответ на задание. Для выполнения задания можно использовать MS EXCEL или алгоритмические языки программирования.

### 5.2.4. Темы докладов, способствующих формированию и оценке знаний компетенции

**ПК-4**

1. Доктрина информационной безопасности РФ 2016 г.
2. ФЗ «Об информации, информационных технологиях и защите информации».
3. ФЗ «О государственной тайне».
4. ФЗ «О коммерческой тайне».
5. ФЗ «О персональных данных».
6. Налоговая и банковская тайны (по НК РФ ст.102 и ФЗ о банках и банковской деятельности ст. 26).
7. Служебная информация ограниченного распространения (по Постановлению Правительства РФ от 3.11.1994 №1233 «Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»).
8. ФЗ «Об электронной подписи».
9. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
10. ФЗ о безопасности критической информационной инфраструктуры РФ (187-ФЗ).

**ПК-9**

1. Симметричное шифрование данных. Основные алгоритмы.
2. Несимметричное шифрование данных. Основные алгоритмы.
3. Современные средства защиты информации компании INFOTECS.
4. Протокол защищенной передачи данных TLS.
5. Протокол защищенной передачи гипертекста HTTPS.

**ПК-8**

1. Вредоносные компьютерные программы. Основные типы, классификация и мероприятия по противодействию (без углубления в антивирусные программы).
2. Антивирусное программное обеспечение.
3. Виды компьютерного мошенничества и способы защиты от него.
4. Служба безопасности организации. Основные функции, задачи. Типовая структура.
5. Промышленный (экономический) шпионаж и способы защиты от него.
6. Брандмауэры (файерволы). Назначение, принцип действия и основные функции. Можно на конкретном примере.
7. Аудит информационной безопасности организации. Цель и задачи. Основные его виды. Основные этапы проведения.

### 5.2.5. Комплексное практическое задание для осуществления практической подготовки по компетенции ПК-4

1. Выбрать организацию (реальную или нет). Описать ее контекст (в соответствии с ГОСТ 27005), который будет необходим для организации процесса менеджмента рисков ИБ:
   - цели и задачи организации;
   - условия, в которых она работает;
   - ограничения, с которыми она сталкивается (финансовые, правовые и другие – смотри ГОСТ);
   - критерии оценки угроз, активов, уязвимостей и рисков ИБ в целом.
2. В соответствии с алгоритмом процесса менеджмента рисков ИБ идентифицировать для этой организации 5 рисков ИБ. Провести их анализ и оценку. В результате получить ранжированный список из 5 рисков.
3. Провести обработку рисков из итого списка, то есть для каждого риска предложить свой наиболее подходящий вариант обработки риска ИБ (название варианта обработки по ГОСТу и конкретное мероприятие).

*Методические указания для выполнения задания:*

А) общий объем текста ответа на задание не более 1 страницы (2400 знаков без пробелов);

Б) Риски, идентифицированные в задании, должны быть разноплановые, то есть активы в них должны быть как аппаратные, так и программные, и информационные; угрозы должны быть как естественные, так и обусловленные человеческим фактором (активные, пассивные, внутренние, внешние и прочие). Все риски должны быть идентифицированы для одной выбранной организации;

В) В контексте организации (в первой части) описывать только то, что будет востребовано и необходимо при выполнении пунктов 2 и 3, то есть при анализе, оценке и обработке 5 названных рисков. Буквально в нескольких словах описываем организацию, чем занимается, в каких условиях работает, какие информационные активы имеет, с какими проблемами с точки зрения ИБ может столкнуться и почему;

Г) Также в первом пункте необходимо пояснить критерии оценки активов, угроз, уязвимостей и рисков в целом, которые будут в дальнейшем применяться. Какой подход вы выбираете: качественный, количественный или комбинированный. Надо охарактеризовать шкалу, которую будете применять для оценки элементов риска. Например, для 5 рисков удобно использовать шкалу от 1 до 5, где 1 – самый низкий уровень опасности (вероятности) элемента риска, а 5 – самый высокий уровень. Вы можете использовать шкалу, которая вам подходит, только надо ее охарактеризовать, чтобы было понятно ее использование в дальнейшем в пункте 2;

Д) Что касается пункта 3, то здесь должны быть задействованы все варианты обработки риска (один вариант обработки для первого риска, другой – для второго, третий – для третьего, четвертый – для четвертого, а для пятого риска – любой вариант обработки или их комбинация). Соответственно, как уже отмечалось, риски должны быть разноплановые и должны предусматривать разные варианты обработки;

Е) Задание индивидуальное, если будут попадаться одинаковые ответы, то оценка будет делиться на количество одинаковых ответов.

## 6. Учебно-методическое и информационное обеспечение дисциплины

### а) основная литература:

1. Щеглов, А. Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. — Москва: Издательство Юрайт, 2020. — 309 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-04732-5. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/449285 (дата обращения: 23.11.2020).
2. Внуков, А. А. Защита информации в банковских системах: учебное пособие для бакалавриата и магистратуры / А. А. Внуков. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2018. — 246 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-01679-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/414083 (дата обращения: 23.11.2020).
3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: Учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Матвеев В.А., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им. Н.И. Лобачевского, 2018. – 182 с. http://www.iee.unn.ru/wp-content/uploads/sites/9/2018/09/Yasenev_posobie_isecurity.pdf

### б) дополнительная литература:

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/450820
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2020. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://urait.ru/bcode/451486
3. Информационная безопасность в экономике: Практикум/ Киселев В.Г., Усков А.В., Ясенев В.Н., Ясенев О.В., Хворенков С.Г.; Под общей редакцией профессора, к.э.н. Ясенева В.Н.- Нижний Новгород: ННГУ, 2013.- 57 с. http://www.iee.unn.ru/wp-content/uploads/sites/9/2014/09/Posobie-po-IB-2013.pdf

### в) программное обеспечение и Интернет-ресурсы:

1. Конституция РФ (http://constitutionrf.ru/);
2. Доктрина информационной безопасности Российской Федерации (утв. утверждена Указом Президента РФ No 646 от 5 декабря 2016 г.) (https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html);
3. Указ правительства РФ No188 об утверждении перечня сведений конфиденциального характера 1997г. (с изм. и доп. от 23 сентября 2005 г., 13 июля 2015 г.) (http://base.garant.ru/10200083/#ixzz4bCt8H6TU);

4. Трудовой кодекс РФ –глава 14 «Защита персональных данных работника» (от 30.12.2001 N 197-ФЗ (ред. от 03.07.2016) (http://www.consultant.ru/document/cons_doc_LAW_34683/);
5. Гражданский кодекс Ч. No4 Раздел 7 «Права на результаты интеллектуальной деятельности и средства индивидуализации» (18 декабря 2006 года N 230-ФЗ) (http://www.consultant.ru/document/cons_doc_LAW_64629/).
6. Программа «Цифровая экономика Российской Федерации» утверждена распоряжением Правительства Российской Федерации от 28 июля 2017 г. № 162-р.
7. Федеральный Закон от 21 июля 1993г. No5485 «О государственной тайне» (Федеральный закон "О внесении изменений в статью 5 Закона Российской Федерации "О государственной тайне" от 15.11.2010 N 299-ФЗ (последняя редакция) (http://www.consultant.ru/document/cons_doc_LAW_106802/);
8. Электронный управляемый курс ЗАЩИТА ИНФОРМАЦИИ https://e-learning.unn.ru/course/view.php?id=4406
9. www.itsec.ru Интернет-журнал «Информационная безопасность».
10. Официальный сайт компании INFOTECS https://infotecs.ru/

## 7.Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: персональными компьютерами, подключенными к сети Интернет, преподавательским ПК с подключенным к нему проектором, экраном для проектора и доской для записей, программным обеспечением всех ПК (ОС Windows, пакеты MS Office, Deductor Academic, различные браузеры для работы во всемирной паутине).

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ФГОС ВО с учетом рекомендаций по направлению 09.04.03 «Прикладная информатика».

Рабочая программа дисциплины утверждена на заседании кафедры ИТИМЭ 14 ноября 2022 г., протокол № 6.

Авторы программы:
к.э.н., профессор В.Н. Ясенев
к.т.н., доцент А.Л. Сочков

Рецензент:
_____ А.Н. Визгунов

Заведующий кафедрой ИТИМЭ
д.э.н., профессор Ю.В. Трифонов