Министерство просвещения ПМР
ГОУ СПО «Тираспольский техникум информатики и права»

IV Республиканский интернет-конкурс
«Лучшая методическая разработка»
среди педагогических работников организаций среднего профессионального образования Приднестровской Молдавской Республики

Номинация
«Лучшая рабочая тетрадь, тетрадь для лабораторных (практических) работ»

РАБОЧАЯ ТЕТРАДЬ
для внеаудиторных самостоятельных работ

по дисциплине ОП.09 «Информационная безопасность»
специальность 09.02.03 «Программирование в компьютерных системах»

Автор: *Гуцул Людмила Михайловна, преподаватель информационных дисциплин ГОУ СПО «Тираспольский техникум информатики и права»*

Тирасполь
2019

Рабочая тетрадь предназначена для выполнения внеаудиторных самостоятельных работ по специальности среднего профессионального образования 09.02.03 «Программирование в компьютерных системах».

Организация: ГОУ СПО «Тираспольский техникум информатики и права».

Разработчик: ***Л.М. Гуцул,*** *преподаватель первой квалификационной категории*.

Аннотация

Одним из важнейших компонентов учебного процесса являются средства обучения.

Наиболее эффективным средством обучения, способствующим более широкому применению на практике различных форм и методов, самостоятельной деятельности обучающихся, являются рабочие тетради.

Целью данной рабочей тетради является усвоение студентами системы знаний и специальных умений и навыков по курсу «Информационная безопасность».

Рабочая тетрадь позволяет студенту работать над изучением материала в удобном для него темпе, достигая конкретные цели учебной и познавательной деятельности, что обеспечивает благоприятные психологические условия, высокий уровень самодисциплины и индивидуальный подход к обучению.

Рабочая тетрадь составлена для дисциплины «Информационная безопасность» в соответствии с требованиями ГОС СПО 09.02.03 «Программирование в компьютерных системах», рабочей программой по учебной дисциплине «Информационная безопасность», предназначена для внеаудиторной самостоятельной работы обучающихся в целях закрепления теоретических знаний и формирования опыта практической деятельности.

Тетрадь включает задания по всем разделам учебной дисциплины: «Основы информационной безопасности», «Уязвимости, угрозы, модели нарушителя», «Средства, используемые злоумышленником» «Методология защиты информации», «Механизмы информационной безопасности», «Оценка защищенности информационной системы».

Выполнение заданий будет способствовать более глубокому усвоению учебного материала, повышению эффективности самостоятельной работы над темами учебной дисциплины, приобретению и систематизации знаний в области информационной безопасности, формированию информационной культуры студентов.

Задания предполагают работу не только с лекционным материалом, учебниками и учебными пособиями, но и предлагают обучающимся, обосновав собственную позицию, дать ответы на некоторые вопросы, что влечет необходимость более глубокого осмысления учебного материала.

Главной целью выполнения заданий с использованием рабочей тетради является получение первичных профессиональных навыков в области информационной безопасности.

Содержание календарно-тематического плана

Наименование разделов, тем дисциплины	Количество часов
Раздел I. Основы информационной безопасности	
Тема 1.1. Основы информационной безопасности	2
Тема 1.2. Классификация конфиденциальной безопасности	2
Тема 1.3. Современная концепция информационной безопасности	2
Раздел II. Уязвимости, угрозы, модели нарушителя	
Тема 2.1. Угрозы информационной безопасности	2
Тема 2.2. Неформальная модель нарушителя	2
Тема 2.3. Каналы утечки и несанкционированный доступ к информации	2
Раздел III. Средства, используемые злоумышленником	
Тема 3.1. Технические средства добывания информации	2
Тема 3.2. Программные средства добывания информации	2
Тема 3.3. Компьютерные вирусы	2
Раздел IV. Методология защиты информации	
Тема 4.1. Принципы построения и направления работ по созданию системы информационной безопасности	2
Тема 4.2. Методы и средства обеспечения ИБ	2
Раздел V. Механизмы информационной безопасности	
Тема 5.1. Идентификация и аутентификация	2
Тема 5.2. Управление доступом в информационной системе. Протоколирование и аудит	2
Тема 5.3. Шифрование. Экранирование	6
Раздел VI. Оценка защищенности информационной системы	
Тема 6.1. Анализ защищенности информационной системы	2
Тема 6.2. Оценка рисков	2
Итого	**36**

Раздел I. ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 1.1. Основы информационной безопасности

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Проанализируйте понятия «безопасность», «безопасность информации», «информационная безопасность», «информационная безопасность личности», используя не менее трех информационных источников. Сформулируйте данные понятия с учетом их смыслоразличительных особенностей.

Безопасность – _____

Безопасность информации – _____

Информационная безопасность – _____

Информационная безопасность личности – _____

Тема 1.2. Классификация конфиденциальной безопасности

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Проанализируйте происхождение понятия «конфиденциальность». Рассмотрите значение этого понятия в латинском и французском языках, а также его значение в словаре В. Даля. Сформулируйте данное понятие с точки зрения этимологии и правовой науки.

Задание 3. Ответьте на вопросы теста.

1) Существует классификация тайн по ... категориям.

Напишите верный вариант ответа (цифра).

Перечислите все категории

2) **По каким трем признакам можно классифицировать информацию, подлежащую защите?**

Выберите верные варианты ответов.

- ☐ по усмотрению владельца;
- ☐ по степени ценности;
- ☐ по принадлежности;
- ☐ по степени конфиденциальности;
- ☐ по содержанию.

3) **Что означает слово „конфиденциальный” в переводе с латинского?**

Выберите верный вариант ответа.

- ○ безопасность;
- ○ защита;
- ○ доверие;
- ○ хранение.

4) **Для любой информационной системы характерны следующие понятия.**

Выберите верные варианты ответов.

- ☐ злоумышленник;
- ☐ непредвиденное обстоятельство;
- ☐ уязвимость;
- ☐ угроза;
- ☐ происшествие.

5) **Защита информации – это ...**

Выберите верный вариант ответа.

- ○ комплекс мероприятий по обеспечению конфиденциальности, целостности, доступности, учета и неотрекаемости информации;
- ○ данные, представленные в виде, пригодном для хранения, обработки и передачи, и представляющие определенную ценность;
- ○ совокупность информационных систем, взаимодействующих между собой, причем одна часть этих систем может иметь интересы, прямо противоположные интересам другой;
- ○ состояние информации, при котором изменять ее могут только уполномоченные лица.

Тема 1.3. Современная концепция информационной безопасности

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Проанализируйте понятие «концепция», используя не менее трех информационных источников. Сформулируйте данное понятие.

Концепция – _____

Задание 3. На основе изученного теоретического материала сформулируйте и запишите концептуальные основы защиты информации.

Основными *целями защиты информации* являются _____

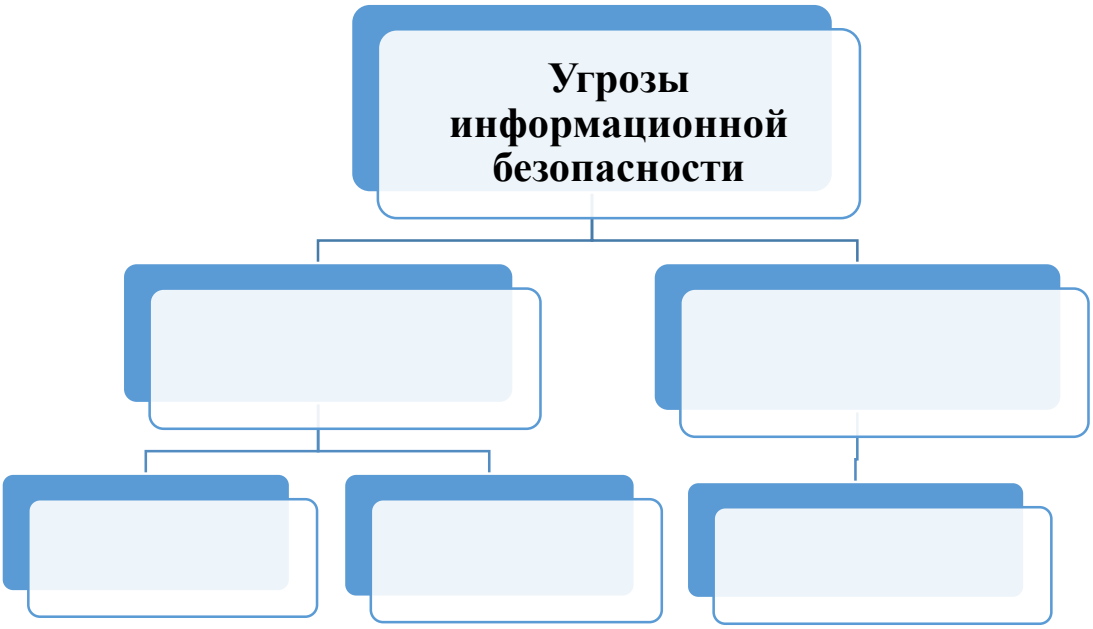
Основными *задачами защиты информации* традиционно считаются _____

Раздел II. УЯЗВИМОСТИ, УГРОЗЫ, МОДЕЛИ НАРУШИТЕЛЯ

Тема 2.1. Угрозы информационной безопасности

📚 **Задание 1.** Изучите теоретический материал по данной теме.

✎ **Задание 2.** Заполните приведенную ниже схему.



✎ **Задание 3.** Дайте определения следующих понятий:

Естественная угроза – _____

_____

_____

_____

Искусственная угроза – _____

_____

_____

_____

Непреднамеренная угроза – _____

_____

_____

_____

Преднамеренная угроза – _____

_____

Утечка информации – _____

Тема 2.2. Неформальная модель нарушителя

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Проанализируйте понятие «нарушитель», используя не менее трех информационных источников. Сформулируйте данное понятие.

Нарушитель – _____

Задание 3. На основе изученного теоретического материала сформулируйте и запишите ***типы нарушителей:***

«Неопытный (невнимательный) пользователь» – _____

«Любитель» – _____

«Мошенник» – _____

«Внешний нарушитель» – _____

«Внутренний злоумышленник» – _____

Тема 2.3. Каналы утечки и несанкционированный доступ к информации

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Проанализируйте понятие «несанкционированный доступ», используя не менее трех информационных источников. Сформулируйте данное понятие.

Несанкционированный доступ – _____

Задание 3. Ответьте на вопросы теста.

1) По отношению к защищаемой информации существуют следующие угрозы. Выберите верный вариант ответа.

- ☐ сокрытие;
- ☐ несанкционированный доступ;
- ☐ утечка;
- ☐ разглашение.

2) Лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства, это ...

Впишите ответ.

3) По источникам появления угрозы подразделяют на:

Выберите верный вариант ответа.

- внешние и внутренние;
- естественные и искусственные;
- пользовательские и сетевые.

4) В зависимости от способов перехвата информации, от физической природы сигналов и среды их распространения технические каналы утечки информации можно разделить на:

Выберите верные варианты ответа.

- дистанционные;
- внешние;
- параметрические;
- электромагнитные;
- электрические.

5) Можно выделить 3 основных мотива нарушений:

Выберите верные варианты ответов.

- действие с целью мести;
- корыстный интерес;
- безответственность;
- самоутверждение.

Раздел III. СРЕДСТВА, ИСПОЛЬЗУЕМЫЕ ЗЛОУМЫШЛЕННИКОМ

Тема 3.1. Технические средства добывания информации

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Ответьте на вопросы теста.

1) Напишите верный вариант ответа.

При облучении лазерным лучом стекол, зеркал, картин и других отражающих поверхностей создается ... канал утечки информации.

_____

2) Выберите верные варианты ответа.

В зависимости от способов перехвата информации, от физической природы сигналов и среды их распространения технические каналы утечки информации можно разделить на:

а) параметрические;

б) внешние;

в) дистанционные;

г) электромагнитные;

д) электрические.

3) Сопоставьте каждому термину его определение:

Неопытный (невнимательный) пользователь	Сотрудник организации, который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные аппаратные и программные средства от своего имени или от имени другого сотрудника
Мошенник	**Внешний нарушитель (злоумышленник)**
Сотрудник организации, который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам организации с превышением своих полномочий, ввода некорректных данных и т.п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства	Постороннее лицо или сотрудник организации, действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор радиоэлектронных способов нарушения безопасности информации, методов и средств взлома систем защиты, характерных для сетей общего пользования
Любитель	**Внутренний злоумышленник**

Сотрудник организации, пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или из „спортивного интереса”. Может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей других пользователей), недостатки в построении системы защиты и доступные ему штатные и нештатные программы	Сотрудник подразделения организации, зарегистрированный как пользователь системы, действующий целенаправленно из корыстных интересов или мести за нанесенную обиду, возможно в сговоре с лицами, не являющимися сотрудниками организации

4) Выберите верный вариант ответа.

По отношению к защищаемой информации существуют следуюшие угрозы:

а) сокрытие;

б) несанкционированный доступ;

в) утечка;

г) разглашение.

5) Напишите правильный ответ.

Лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т.п.) и использующее для этого различные возможности, методы и средства, это ...

_____

Тема 3.2. Программные средства добывания информации

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Заполните таблицу «*Эволюция компьютерных вирусов*».

Автор	Название компьютерного вируса	Краткое описание механизма работы вируса
Басит Фарук Алви (Basit Farooq Alvi) и Ам-джад Фарук Алви (Amjad Farooq Alvi)	BRAIN (1986)	Brain («Мозг») был первым вирусом, удар которого был направлен на компьютеры под управлением популярной в то время операционной системы Microsoft MS-DOS. Вирус Brain инфицировал загрузочный сектор 5-дюймовых дискет объемом 360 Кбайт (уже мало кто помнит такие флоппики). После заражения вирус постепенно заполнял все неиспользуемое пространство дискеты, делая невозможным дальнейшее ее использование

Роберт Таппан Моррис (Robert Tappan Morris)	MORRIS (1988)	

Проанализируйте заполненную таблицу. Почему стало возможным распространение вирусов? Выскажите письменно свое мнение по этому вопросу.

Тема 3.3. Компьютерные вирусы

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Ответьте на вопросы теста.

1) Выберите верный вариант ответа для заполнения пропуска в утверждении.

Универсальным средством защиты от внедрения вредоносной программы является создание (.....) компьютера.

а) изолированного;

б) портативного;

в) персонального.

2) Сопоставьте классы антивирусных продуктов и характеристики их работы:

Эвристический анализ	Данная технология работает с помощью системного драйвера, который перехватывает все запросы на запись на жесткий диск и вместо выполнения записи на реальный жесткий диск выполняет запись в специальную дисковую область – буфер. Таким образом, даже в том случае, если пользователь запустит вредоносное программное обеспечение, оно проживет не далее чем до очистки буфера, которая по умолчанию выполняется при выключении компьютера
Эмуляция кода	Технология анализа поведения основывается на перехвате всех важных системных функций или установке т.н. мини-фильтров, что позволяет отслеживать всю активность в системе пользователя. Технология поведенческого анализа позволяет оценивать не только единичное действие, но и цепочку действий, что многократно повышает эффективность противодействия вирусным угрозам. Также, поведенческий анализ является технологической основой для целого класса программ – поведенческих блокираторов (HIPS – Host-based Intrusion Systems)
Анализ поведения	Метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы
Sandboxing (Песочница) – ограничение привилегий выполнения	Технология эмуляции позволяет запускать приложение в среде эмуляции, эмулируя поведение ОС или центрального процессора. При выполнении приложения в режиме эмуляции приложение не сможет нанести вреда системе пользователя, а вредоносное действие будет детектировано эмулятором
Виртуализация рабочего окружения	Технология эвристического анализа позволяет на основе анализа кода выполняемого приложения, скрипта или макроса обнаружить участки кода, отвечающие за вредоносную активность
Обнаружение, основанное на сигнатурах	Данная технология работает по принципу ограничения активности потенциально вредоносных приложений таким образом, чтобы они не могли нанести вреда системе пользователя. Ограничение активности достигается за счет выполнения неизвестных

	приложений в ограниченной среде – собственно песочнице, откуда приложение не имеет прав доступа к критическим системным файлам, веткам реестра и другой важной информации. Технология ограничения привилегий выполнения является эффективной технологией противодействия современным угрозам, но, следует понимать, что пользователь должен обладать знаниями, необходимыми для правильной оценки неизвестного приложения

3) Восстановите порядок действий защиты от программных закладок и других программных средств добывания информации:

а) (_) выявить вредоносную программу;

б) (_) удалить вредоносную программу;

в) (_) не допустить внедрения вредоносную программу в компьютерную систему.

4) Сопоставьте термины и их определения:

Файловые вирусы	Распространяются по компьютерным сетям
Файлово-загрузочные вирусы	Внедряются главным образом в исполняемые модули, но могут внедряться и в другие типы файлов
Сетевые вирусы	Внедряются в загрузочный сектор диска
Загрузочные вирусы	Заражают как файлы, так и загрузочные сектора дисков

5) Вставьте пропущенное слово в определении.

Вредоносная программа, выполняющая несанкционированные и недокументированные действия, состоящая из двух частей – серверной и клиентской – это ... программа.

_____

Раздел IV. МЕТОДОЛОГИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Тема 4.1. Принципы построения и направления работ по созданию системы информационной безопасности

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Сопоставьте принципы по созданию системы информационной безопасности и их характеристики.

Принцип системности	Предполагает согласованное применение разнородных средств при построении целостной СИБ, перекрывающей все существенные каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов
Принцип комплексности	Суть принципа состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможность ее преодоления даже разработчику защиты
Принцип непрерывности защиты	Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень безопасности. Данный принцип подразумевает возможность изменения уровня защищенности в зависимости от изменения внешних условий и требований с течением времени
Принцип разумной достаточности	Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе законных пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций
Принцип гибкости управления и применения	ЗИ – это не разовое мероприятие, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации
Принцип открытости алгоритмов и механизмов защиты.	Системный подход предполагает необходимость учета всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, значимых для понимания и решения проблемы обеспечения безопасности
Принцип простоты применения защитных мер и средств	Создать абсолютно непреодолимую систему безопасности принципиально невозможно. Важно правильно выбрать тот достаточный уровень защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми

Тема 4.2. Методы и средства обеспечения ИБ

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Кратко опишите базу своей производственной практики. Перечислите мероприятия, обеспечивающие административный и программно-технический уровни информационной безопасности, с которыми вам пришлось сталкиваться на базе производственной практики.

Раздел V. МЕХАНИЗМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 5.1. Идентификация и аутентификация

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Заполните таблицу *«Аутентификация с помощью биометрических данных»*.

Физиологические/поведенческие особенности	**Особенности работы с биометрическими данными**
Отпечатки пальцев	

Тема 5.2. Управление доступом в информационной системе. Протоколирование и аудит

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Какие задачи реализуются с использованием протоколирования и аудита?

1) _____

2) _____

3) _____

Задание 3. Перечислите основные события, безусловно требующие протоколирования:

1) _____

2) _____

3) _____

4) _____

5) _____

Тема 5.3. Шифрование. Экранирование

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Решите задачи по шифрованию данных.

1.Зашифровать словосочетание «Съешь же ещё этих мягких французских булок, да выпей чаю», используя шифр Цезаря. Шифрование с использованием ключа K = 3.

2.Зашифровать словосочетание «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ», используя шифр «Вертикальной перестановки» и ключ «ДЯДИНА».

3.Зашифровать словосочетание «Я мыслю, следовательно, существую», используя шифр «Квадрат Полибия».

Раздел VI. ОЦЕНКА ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Тема 6.1. Анализ защищенности информационной системы

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Письменно дополните последовательность мероприятий по анализу защищенности.

Анализ защищенности ИС в общем случае включает в себя следующие этапы работы:

1. Инициирование и планирование:

1) _____
2) _____
3) _____
4) _____
5) _____

2. Обследование, документирование и сбор информации:

1) _____
_____
2) _____
_____
3) _____
_____
4) _____
_____

3. Анализ полученных данных и уязвимостей:

1) _____
_____
2) _____
_____
3) _____
_____
4) _____
_____
5) _____
_____
6) _____
_____

4. Выработка рекомендаций:

1) _____
_____
2) _____
_____
3) _____
_____

5. Подготовка отчетных документов.

Тема 6.2. Оценка рисков

Задание 1. Изучите теоретический материал по данной теме.

Задание 2. Заполните таблицу «*Инструментальные средства анализа защищенности*».

Название инструментального средства	**Примеры программ**
Сетевые сканеры безопасности	
	Security Benchmarks, CIS Scoring Tools, CIS Router Audit Toolkit, Windows Security Templates, Security Analysis Tool
Сетевые взломщики паролей	
	host, showmount, traceout, rusers, finger, ping
Средства инвентаризации и сканеры ресурсов сети	
	tcpdump, wireshark