

**Калужский филиал
Частное учреждение профессионального образования
Юридический полицейский колледж**



УТВЕРЖДАЮ
Директор Калужского филиала
ЧУ ПО ЮПК
Л.А. Крикалова
2024 г.

**РАБОЧАЯ ПРОГРАММА
учебной дисциплины ЕН.03
«Защита информации»**

для обучающихся на базе основного общего образования
по специальности:

40.02.01 «Право и организация социального обеспечения».

ПРИНЯТО

Методическим советом
Юридического полицейского колледжа
Протокол № ___ от _____ 2024 года

РАССМОТРЕНО

на заседании Педагогического совета
Протокол № ___ от _____ 2024 года

Разработчик:

Учебно-методический отдел ЮПК

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ	стр. 8
2. СТРУКТУРА И ПРИМЕРНОЕ СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ	10
3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ	15
4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ	16

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ «Защита информации»

1.1. Область применения рабочей программы

Рабочая программа учебной дисциплины «Защита информации» является вариативной частью общеобразовательной подготовки студентов в учреждениях СПО по специальностям:

- 40.02.01 «Право и организация социального обеспечения»;
- 40.02.02 «Правоохранительная деятельность».

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Защита информации» относится к вариативной части математического и общего естественно-научного цикла дисциплин по специальностям:

- 40.02.01 «Право и организация социального обеспечения»;
- 40.02.02 «Правоохранительная деятельность».

1.3. Цели и задачи учебной дисциплины – требования к результатам освоения учебной дисциплины:

В результате освоения учебной дисциплины студент должен:

знать:

- содержание понятий "утрата информации", "потеря информации", "утечка информации", "форс-мажор", "аппаратная зависимость утраты информации", "влияние человеческого фактора на утрату информации",
- пути утраты информации,
- влияние аппаратной зависимости на возможность утраты информации,
- влияние человеческого фактора на возможность утраты информации;
- меры по защите информации при работе на локальном компьютере,
- меры по защите информации при работе компьютера в сети,
- методы защиты информации от форс-мажорных обстоятельств,
- пути аппаратно зависимой потери информации,
- сбои аппаратного и программного характера,
- меры для предотвращения аппаратно зависимой потери информации;
- способ представления данных в компьютере,
- систему хранения информации на дисках,
- причины сохранения на дисках удалённых файлов,
- методику восстановления диска и данных;
- уязвимости локального компьютера,
- способы защиты файлов и папок,
- применение архиваторов для скрытия и защиты файлов,
- способы уничтожения удаленного и исправленного текста,
- современные утилиты очистки диска;
- содержание понятия "компьютерный вирус",
- разновидности компьютерных вирусов,
- способы проникновения вирусов в компьютер,
- действия, выполняемые вирусами,
- методы и способы защиты от вирусов,
- современные антивирусные программы;
- опасности при работе в сети,
- о системах защиты, используемых для компьютера, подключённого к сети,
- основные элементы сетевой безопасности,
- способы защиты электронной почты,
- средства сохранения конфиденциальности при работе в сети Интернет;
- содержание понятия "шифрование",

- форматы представления и форматы кодирования данных,
- шифрование с открытым и закрытым ключами,
- современные программы, используемые для шифрования,
- способы шифрования данных на локальном компьютере,
- способы шифрования почтовых сообщений,
- ключевую роль человеческого фактора в проблеме защиты информации,
- меры по предотвращению утраты информации в случае неверных действий пользователя,
- меры по предотвращению утечки информации через знания персонала,
- меры по предотвращению утраты информации при несанкционированном физическом доступе к компьютеру.
- содержание понятий "хакинг", "хакер", "удалённая атака",
- способы защиты вычислительной системы и информации от удалённых хакерских атак;
- современные технические средства защиты вычислительных систем,
- способы физической защиты вычислительных систем.

уметь:

- использовать современные программные и аппаратные средства для создания резервных копий данных.
- - проводить минимальное обслуживание системы стандартными диагностическими программами, входящими в состав утилит операционных систем.
- пользоваться программой-утилитой для восстановления данных.
- защищать локальный компьютер при помощи системы паролей,
- защищать файлы и папки при помощи системы паролей,
- обеспечивать защиту локального включённого компьютера при временном отсутствии на рабочем месте,
- обеспечивать защиту локального выключенного компьютера,
- применять какое-либо современное программное средство для уничтожения удалённого и исправленного теста,
- пользоваться какой-либо современной утилитой очистки диска.
- устанавливать элементы обеспечения сетевой безопасности компьютера,
- устанавливать системы защиты электронной почты.
- пользоваться современной антивирусной программой.
- пользоваться современной программой для шифрования данных,
- пользоваться программой для шифрования почтовых сообщений.
- содержание понятия "перехват информации",
- технические и программные средства, используемые для перехвата,
- технические и программные средства, используемые для защиты от перехвата,
- меры для предотвращения утечки информации при перехвате,
- методику действий при обнаружении перехвата;
- обеспечить защиту информации при обнаружении перехвата.
- настроить защиту вычислительной системы от удалённых хакерских атак.

1.4. Количество часов на освоение программы учебной дисциплины:

максимальной учебной нагрузки студента 68 часов, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося 8 часа;
- обязательной аудиторной практической работы обучающегося, в т.ч. лабораторных занятий 2 часа;
- самостоятельной работы студента 60 часов.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ**2.1. Объем учебной дисциплины и виды учебной работы**

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	68
Обязательная аудиторная учебная нагрузка (всего)	8
в том числе:	
практические занятия	2
лабораторные занятия	
Самостоятельная работа обучающегося (всего)	60
в том числе:	
внеаудиторная самостоятельная работ: работа над материалом рабочей тетради «Защита информации», конспектом лекций	60
Итоговая аттестация в форме комплексного экзамена	

2.2. Тематический план и содержание учебной дисциплины «Защита информации»

Наименование разделов и тем	Содержание учебного материала, лабораторные работы и практические занятия, самостоятельная работа обучающихся	Уровень освоения
1	2	3
Раздел 1.	Информация и её защита	1,2
Тема 1.1. Понятие, цели и направление защиты информации.	<p>Основные понятия информационной безопасности. Интересы субъектов, связанных с использованием информационных ресурсов. Определение понятия Защита информации. Угрозы безопасности информации. Объектами угроз. Виды возможных ущербов (потерь). Виды защиты информации. Основные виды защищаемой информации. Правовые вопросы обеспечения защиты данных.</p> <p>На самостоятельное изучение: Правовые вопросы обеспечения защиты данных.</p>	
Тема 1.2. Форс-мажорные обстоятельства и предотвращение утраты информации.	<p>Форс-мажорные обстоятельства. Основные этапы разработки плана защиты ИВС. Особенности воздействия на ИВС различных факторов Метод защиты от форс-мажорных обстоятельств – резервное копирование системы. Классификация путей утраты информации.</p> <p>На самостоятельное изучение: Традиционные каналы утечки информации.</p>	
Тема 1.3. Предотвращение аппаратно-зависимой утраты информации.	<p>Практическая работа 1. Предотвращение аппаратно-зависимой утраты информации. Пути аппаратно зависимой утраты информации: физическое разрушение или нарушение аппаратуры, сбой аппаратного характера, сбой программного характера. Два типа профилактических мероприятий: активные и пассивные. Пассивные профилактические меры – создание приемлемых для компьютера общих внешних условий. Влияние нагревания и охлаждения, циклов включения и выключения, электростатических разрядов, помех в сети электропитания, радиочастотных помех, окружающей среды на работу компьютера и меры профилактики.</p> <p>Лабораторная работа 1. Предотвращение аппаратно-зависимой утраты информации. Меры активного профилактического обслуживания: резервное копирование системы, чистка, дефрагментация файлов, антивирусные программы.</p> <p>На самостоятельное изучение: Сроки службы различных компонентов компьютера.</p>	
РАЗДЕЛ 2.	ПРЕДОТВРАЩЕНИЕ ПОТЕРИ ИНФОРМАЦИИ	1,2
Тема 2.1. Восстановление диска и данных.	Способ представления данных в компьютере. Система хранения информации на дисках. Причины сохранения удалённых файлов на дисках. Восстановление данных. Способы восстановления данных. Восстановление удаленных данных файловой системы.	

	На самостоятельное изучение: Дефрагментация диска	
Тема 2.2. Предотвращение утраты информации на локальном компьютере.	Меры предотвращения утечки информации на локальном компьютере для организации. Правила и приемы безопасной работы на компьютере. Технические меры защиты информации на локальном компьютере. Организационные меры защиты информации на локальном компьютере. Защита компьютера паролем. Требования к надежному паролю. Рекомендации по защите паролей.	
	На самостоятельное изучение: Создать различные пароли и оценить их надежность.	
Тема 2.3. Предотвращение утраты информации при работе компьютера в сети.	Практическая работа 2. Предотвращение утраты информации при работе компьютера в сети. Основные элементы сетевой безопасности. Задачи, которые решают системы сетевой безопасности. Методы защиты в сети. Рекомендации по защите паролей. Средства защиты информации в Интернете. Организационные меры. Файлы cookie. Программные средства анонимной работы.	
	Лабораторная работа 2. Предотвращение утраты информации при работе компьютера в сети. Поиск и удаление записей о сетевой деятельности. Файлы cookie.	
	На самостоятельное изучение: Программные средства анонимной работы.	
РАЗДЕЛ 3.	ЗАЩИТА ИНФОРМАЦИИ	1,2
Тема 3.1 Защита информации от компьютерных вирусов.	Понятие вредоносных программ. Виды вредоносных программ. Вирусы и трояны. Этапы жизненного цикла компьютерных вирусов. Способы проявления компьютерных вирусов. Классификации компьютерных вирусов. Меры и средства защиты от вредоносных программ. Правила защиты от вредоносных программ.	
	На самостоятельное изучение: Потери организаций от компьютерных вирусов.	
Тема 3.2. Криптографические способы защиты информации.	Практическая работа 3. Криптографические способы защиты информации. Криптография. Методы криптографического преобразования информации. Шифрование. Стенография. Кодирование. Сжатие. Методы шифрования. Причины отсутствия повсеместного шифрования. Области применения криптографии.	
	На самостоятельное изучение: Области применения криптографии.	

<p>Тема 3.3 Предотвращение перехвата информации.</p>	<p>Практическая работа 4 Предотвращение перехвата информации. Перехват информации. Рекомендации по противодействию перехвату информации. Технические способы организации противодействия утечки информации. Перехват информации с помощью электронных средств. Меры для предотвращения утечки информации при перехвате. Программы мониторинга работы в сети.</p> <p>На самостоятельное изучение: Оценка различных способов перехвата информации</p>	
<p>Тема 3.4 Человеческий фактор и предотвращение утраты информации.</p>	<p>Практическая работа 5. Человеческий фактор и предотвращение утраты информации. Ключевая роль человеческого фактора в проблеме защиты информации. Определение потенциального нарушителя. Классификация нарушителей. Мотивы действий нарушителей. Утечки информации через персонал.</p> <p>На самостоятельное изучение: Оценить различные категории нарушителей.</p>	
<p>Тема 3.5 Удалённая атака. Способы защиты вычислительной системы от удалённых атак «хакеров».</p>	<p>Практическая работа 6. Удалённая атака. Способы защиты вычислительной системы от удалённых атак «хакеров». Классификация атак. Типовые удаленные атаки. Технологии обнаружения атак. Методы анализа сетевой информации. Компьютерные преступления. Виды киберпреступлений.</p> <p>На самостоятельное изучение: Оценить вред, приносимый различными компьютерными преступлениями.</p>	
<p>Тема 3.6 Технические и физические средства защиты информации.</p>	<p>Практическая работа 7. Технические и физические средства защиты информации. Технические средства защиты вычислительных систем. Устройства пассивной и активной защиты, их краткая характеристика. Программно-технические средства защиты информации. Организация физической защиты вычислительных систем. Основные компоненты, используемые при организации физической защиты. Устройства пассивной и активной защиты</p> <p>На самостоятельное изучение: Сравнить различные меры защиты информации по критерию эффективности.</p>	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1 – ознакомительный (узнавание ранее изученных объектов, свойств);

2 – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством)

3. УСЛОВИЯ РЕАЛИЗАЦИИ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Требования к минимальному материально-техническому обеспечению

Оборудование учебного кабинета:

1. посадочные места по количеству обучающихся;
2. рабочее место преподавателя;
3. аудиторная доска для письма.

Технические средства обучения:

1. видео-аудио техника;
2. юридическая литература;
3. раздаточный материал;
4. технические средства комфортного доступа обучающихся с ограниченными возможностями здоровья и инвалидов к возможностям получения образования (ассистирующие средства и технологии), включая специализированные компьютерные инструменты образования, ориентированные на удовлетворение особых образовательных потребностей.

3.2. Информационное обеспечение обучения

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы.

Основная литература:

Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-473-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/118932>. – Режим доступа: по подписке.

Дополнительная литература:

Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учеб. пособие / В.Ф. Шаньгин. — Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. — 416 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0754-2. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1009605> – Режим доступа: по подписке.

Серова, Г. А. Информационные технологии в юридической деятельности : учебное пособие / Г.А. Серова. — Москва : ИНФРА-М, 2021. — 241 с. — (Среднее профессиональное образование). - ISBN 978-5-16-015946-1. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1199884>. – Режим доступа: по подписке.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий.

Результаты обучения (освоенные умения, усвоенные знания)	Формы и методы контроля и оценки результатов обучения
<p>В результате освоения учебной дисциплины студент должен:</p> <p>знать:</p> <ul style="list-style-type: none"> • содержание понятий "утрата информации", "потеря информации", "утечка информации", "форс-мажор", "аппаратная зависимость утраты информации", "влияние человеческого фактора на утрату информации", • пути утраты информации, • влияние аппаратной зависимости на возможность утраты информации, • влияние человеческого фактора на возможность утраты информации; • меры по защите информации при работе на локальном компьютере, • меры по защите информации при работе компьютера в сети, • методы защиты информации от форс-мажорных обстоятельств, • пути аппаратно зависимой потери информации, • сбои аппаратного и программного характера, • меры для предотвращения аппаратно зависимой потери информации; • способ представления данных в компьютере, • систему хранения информации на дисках, • причины сохранения на дисках удалённых файлов, • методику восстановления диска и данных; • уязвимости локального компьютера, • способы защиты файлов и папок, • применение архиваторов для скрытия и защиты файлов, • способы уничтожения удаленного и исправленного текста, • современные утилиты очистки диска; • содержание понятия "компьютерный вирус", • разновидности компьютерных вирусов, • способы проникновения вирусов в компьютер, • действия, выполняемые вирусами, • методы и способы защиты от вирусов, • современные антивирусные программы; • опасности при работе в сети, • о системах защиты, используемых для компьютера, подключённого к сети, • основные элементы сетевой безопасности, 	<ol style="list-style-type: none"> 1. Интерпретация результатов наблюдений за деятельностью обучающегося в процессе освоения образовательной программы. 2. Стартовая диагностика подготовки обучающихся по школьному курсу информатики; выявление мотивации к изучению нового материала. 3. Текущий контроль в форме: <ul style="list-style-type: none"> - оценки практических занятий и защиты лабораторных работ; - контрольных работ по темам разделов дисциплины; - тестирования; - домашней работы; - отчёта по проделанной внеаудиторной самостоятельной работе согласно инструкции (представление пособия, презентации /буклета, информационное сообщение). 4. Рубежный контроль по темам «Защита информации, «Форс-мажорные обстоятельства и предотвращение утраты информации». 5. Итоговая аттестация в форме комплексного экзамена.

- способы защиты электронной почты,
- средства сохранения конфиденциальности при работе в сети Интернет;
- содержание понятия "шифрование",
- форматы представления и форматы кодирования данных,
- шифрование с открытым и закрытым ключами,
- современные программы, используемые для шифрования,
- способы шифрования данных на локальном компьютере,
- способы шифрования почтовых сообщений,
- ключевую роль человеческого фактора в проблеме защиты информации,
- меры по предотвращению утраты информации в случае неверных действий пользователя,
- меры по предотвращению утечки информации через знания персонала,
- меры по предотвращению утраты информации при несанкционированном физическом доступе к компьютеру.
- содержание понятий "хакинг", "хакер", "удалённая атака",
- способы защиты вычислительной системы и информации от удалённых хакерских атак;
- современные технические средства защиты вычислительных систем,
- способы физической защиты вычислительных систем.

уметь:

- использовать современные программные и аппаратные средства для создания резервных копий данных.
- - проводить минимальное обслуживание системы стандартными диагностическими программами, входящими в состав утилит операционных систем.
- пользоваться программой-утилитой для восстановления данных.
- защищать локальный компьютер при помощи системы паролей,
- защищать файлы и папки при помощи системы паролей,
- обеспечивать защиту локального включённого компьютера при временном отсутствии на рабочем месте,
- обеспечивать защиту локального выключенного компьютера,
- применять какое-либо современное программное средство для уничтожения удалённого и исправленного теста,

<ul style="list-style-type: none"> • пользоваться какой-либо современной утилитой очистки диска. • устанавливать элементы обеспечения сетевой безопасности компьютера, • устанавливать системы защиты электронной почты. • пользоваться современной антивирусной программой. • пользоваться современной программой для шифрования данных, • пользоваться программой для шифрования почтовых сообщений. • содержание понятия "перехват информации", • технические и программные средства, используемые для перехвата, • технические и программные средства, используемые для защиты от перехвата, • меры для предотвращения утечки информации при перехвате, • методику действий при обнаружении перехвата; • обеспечить защиту информации при обнаружении перехвата. • настроить защиту вычислительной системы от удалённых хакерских атак. 	
--	--

Оценка индивидуальных образовательных достижений по результатам текущего контроля производится в соответствии с универсальной шкалой (таблица).

Процент результативности (правильных ответов)	Качественная оценка индивидуальных образовательных достижений	
	Балл (отметка)	Вербальный аналог
90-100	5	Отлично
80-89	4	Хорошо
70-79	3	Удовлетворительно
Менее 70	2	Неудовлетворительно