МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

Факультет криминальной милиции

Кафедра информационного права

УТВЕРЖДАЮ
Начальник кафедры
информационного права
факультета криминальной
милиции
полковник милиции
Д.Н.Лахтиков
30.06.2023

Регистрационный № 2/19-177

МЕТОДИКА ПРЕПОДАВАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)»

для специальностей 6-05-0421-01 (1-24 01 02) Правоведение,
6-05-0421-03 (1-24 01 03) Экономическое право

РАЗРАБОТЧИКИ (АВТОРЫ):

П.Л.Боровик, доцент кафедры информационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь», кандидат юридических наук, доцент

РЕЦЕНЗЕНТ:

Н.М.Бобович, доцент кафедры информационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь», кандидат технических наук, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой информационного права факультета криминальной милиции протокол № ___ от _____ 2023 г.

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

На изучение учебной дисциплины «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» в соответствии с учебными планами для специальностей 6-05-0421-01 (1-24 01 02) Правоведение, 6-05-0421-03 (1-24 01 03) Экономическое право предусмотрено 98 часов, в том числе:

Дневная форма получения высшего образования

48 – аудиторных часов, из которых 10 часов – лекции, 10 часов – семинарские занятия, 28 часов – практические занятия.

Распределение общего и аудиторного времени по семестрам и видам занятий составляет:

7 семестр: общее количество часов – 98, количество аудиторных часов – 48, из которых 10 часов – лекции, 10 часов – семинарские занятия, 28 часов – практические занятия.

Форма промежуточной аттестации по учебной дисциплине: экзамен в 7 семестре, количество зачетных единиц – 5.

На изучение учебной дисциплины «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» в соответствии с учебными планами для специальностей 6-05-0421-01 (1-24 01 02) Правоведение, 6-05-0421-03

(1-24 01 03) Экономическое право предусмотрено 104 часа, в том числе:

Заочная форма получения высшего образования (для наборов 2022 и 2023 годов):

Срок получения высшего образования – 3 года: общее количество часов – 98, количество аудиторных часов – 12, из которых 4 часа – лекции, 8 часов – практические занятия.

Распределение общего и аудиторного времени по семестрам и видам занятий составляет:

5 семестр: общее количество часов – 49 часов, количество аудиторных часов – 2, из которых 2 часа – лекции.

6 семестр: общее количество часов – 49 часов, количество аудиторных часов – 12, из которых 2 часа – лекции, 8 часов – практические занятия.

Форма промежуточной аттестации по учебной дисциплине: экзамен в 6 семестре, количество зачетных единиц – 3.

Заочная форма получения высшего образования

Срок получения высшего образования – 3 года (для наборов 2020 и 2021 годов): общее количество часов – 98, количество аудиторных часов – 12, из которых 4 часа – лекции, 8 часов – практические занятия.

Распределение общего и аудиторного времени по семестрам и видам занятий составляет:

9 семестр: общее количество часов – 49 часов, количество аудиторных часов – 2, из которых 2 часа – лекции.

10 семестр: общее количество часов – 49 часов, количество аудиторных часов – 12, из которых 2 часа – лекции, 8 часов – практические занятия.

Форма промежуточной аттестации по учебной дисциплине: экзамен в 10 семестре, количество зачетных единиц – 3.

Заочная форма получения высшего образования (для профилизаций «Судебно-прокурорско-следственная деятельность», «Административно-правовая деятельность», наборы 2021 и 2022 годов):

Срок получения высшего образования – 5 лет: общее количество часов – 98, количество аудиторных часов – 12, из которых 2 часа – лекции, 10 часов – практические занятия.

Распределение общего и аудиторного времени по семестрам и видам занятий составляет:

9 семестр: общее количество часов – 49 часов, количество аудиторных часов – 8, из которых 2 часа – лекции, 6 часов – практические занятия.

10 семестр: общее количество часов – 49 часов, количество аудиторных часов – 4, из которых 4 часов – практические занятия.

Форма промежуточной аттестации по учебной дисциплине: экзамен в 10 семестре, количество зачетных единиц – 3.

Заочная форма получения высшего образования (для профилизации «Административно-правовая деятельность», набор 2020 года):

Срок получения высшего образования – 5 лет: общее количество часов – 144, количество аудиторных часов – 16, из которых 8 часов – лекции, 8 часов – практические занятия.

Распределение общего и аудиторного времени по семестрам и видам занятий составляет:

9 семестр: общее количество часов – 49 часов, количество аудиторных часов – 12, из которых 8 часа – лекции, 4 часов – практические занятия.

10 семестр: общее количество часов – 49 часов, количество аудиторных часов – 4, из которых 4 часов – практические занятия.

Форма промежуточной аттестации по учебной дисциплине: экзамен в 10 семестре, количество зачетных единиц – 5.

Цель изучения дисциплины – усвоение обучающимися приемов и методов защиты информации, основ противодействия киберпреступлениям, а также подготовка к выполнению задач по обнаружению и фиксации компьютерной информации в контексте будущей профессиональной деятельности.

Задачами учебной дисциплины «Комплексная защита информации и противодействие киберпреступности (ПКиОЗИ)» являются:

освоение обучающимися на основе междисциплинарного подхода системных знаний о правовых, организационных мерах по защите информации в правоохранительных органах; методах и средствах обеспечения безопасности информации; аппаратных и программных средствах защиты информации; особенностях обнаружения и анализа компьютерной информации;

формирование у обучающихся обобщенных умений применения информационно-коммуникационных технологий в решении профессиональных задач, в том числе умений пользоваться информационными ресурсами, современными программными и

аппаратными средствами, используемыми в правоохранительной деятельности;

формирование способности к непрерывному саморазвитию, повышению своей квалификации и реализации инновации в профессиональной деятельности.

Решение поставленных задач осуществляется в ходе проведения лекционных, семинарских и практических занятий по учебной дисциплине «Противодействие киберпреступности и основы защиты информации» с применением и оптимальным сочетанием разнообразных методов преподавания.

Необходимые теоретические знания о каналах утечки информации и безопасности информационных систем, аппаратном и программном обеспечении защищенных компьютерных систем, а также об основах противодействия компьютерной преступности обучающиеся поэтапно получают на лекционных и семинарских занятиях.

Навыки работы со средствами компьютерной техники, овладение методами и средствами решения задач в области правоохранительной деятельности с использованием современных информационных технологий приобретаются обучающимися на практических занятиях по учебной дисциплине.

2. ОСНОВНЫЕ МЕТОДЫ ПРОВЕДЕНИЯ УЧЕБНЫХ ЗАНЯТИЙ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Методика проведения лекционных занятий

В соответствии с учебной программой по учебной дисциплине «Комплексная защита информации и противодействие киберпреступности (ПКиОЗИ)» предусмотрено проведение пяти лекционных занятий по темам «Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь» (тема 1), «Каналы утечки информации и безопасность информационных систем» (тема 2), «Аппаратное и программное обеспечение защищенных компьютерных систем» (тема 3), «Основы противодействия киберпреступности» (тема 4) и «Компьютерная информация: обнаружение и анализ» (тема 5).

Структура лекционных занятий состоит из трех основных элементов: введения, основной части и заключения.

Проведение лекции

Вводная часть (до 10 мин)

Занятие начинается с принятия преподавателем доклада командира о готовности учебной группы (курса) к занятию, выборочной проверки присутствующих. Затем преподаватель сообщает о начале изучения новой учебной темы, показывает ее связь со смежными юридическими дисциплинами, доводит требования, предъявляемые к обучающимся, по ведению конспектов, посещению занятий и консультаций.

После этого объявляется тема и цели занятия, перечисляются вопросы, которые будут освещены в лекции, рекомендуется литература и нормативные правовые акты для самостоятельного изучения (по усмотрению преподавателя цели и учебные вопросы могут быть обозначены в завершении вводного слова, а перечисление литературы и нормативных правовых актов по теме – в конце лекции).

Преподаватель обозначает актуальность и значимость заявленной темы в практической деятельности сотрудников органов внутренних дел, демонстрирует взаимосвязь данной темы с положениями других учебных тем.

Основная часть

В основной части занятия преподаватель излагает систематизированные научные знания по учебной дисциплине через последовательное рассмотрение учебных вопросов, раскрывает ключевые наиболее сложные положения изучаемой темы. Преподаватель освещает содержание учебных вопросов посредством сочетания теоретического материала (раскрытия концептуальных основ, понятий и идей современной науки) с примерами из практической деятельности

оперативных подразделений органов внутренних дел. Излагаемый материал может сопровождаться демонстрацией слайдов, видеосюжетов, компьютерной графики и т. д. Порядок применения технических средств обучения (учебной доски, мультимедийного проектора, компьютера и др.) преподаватель определяет самостоятельно с учетом имеющихся технических возможностей.

Основной вид лекции, используемый в преподавании учебной дисциплины «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)», является *лекция-информация*, предполагающая поэтапное рассмотрение преподавателем вопросов темы в соответствии с учебной программой по учебной дисциплине.

Преобладающими методами проведения лекционных занятий по учебной дисциплине «Комплексная защита информации и противодействие киберпреступности» являются ***вербальные (словесные) методы***, такие как рассказ и объяснение, в сочетании с ***визуальными (наглядными) методами***, представленными, иллюстрацией и демонстрацией.

Заключительная часть (до 10 мин)

В заключительной части лекции преподаватель делает краткие выводы, перечисляет литературу и нормативные правовые акты (если это не сделано ранее), для самостоятельного изучения по прочитанной теме. Затем преподаватель предлагает обучающимся задать вопросы по теме и отвечает на них. После этого он сообщает обучающимся место и вид следующего занятия, а при необходимости может дать им конкретные задания (законспектировать инструкцию, подготовить доклады по учебным вопросам следующего занятия и т. п.).

В завершение преподаватель объявляет об окончании занятия[1].

Особенности методики проведения лекционных занятий по темам (по усмотрению преподавателя):

Тема 1. «Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь». Рассказ, объяснение, демонстрация в форме компьютерной презентации (по усмотрению преподавателя), представление изучаемого материала в сравнительных или классификационных таблицах, метод опорных схем.

Тема 2. «Каналы утечки информации и безопасность информационных систем». Рассказ, объяснение, демонстрация в форме компьютерной презентации, представление изучаемого материала в сравнительных или классификационных таблицах, метод опорных схем.

[1] Указанная методика используется при чтении лекций по всем темам.

Тема 3. «Аппаратное и программное обеспечение защищенных компьютерных систем». Рассказ, объяснение, демонстрация в форме компьютерной презентации, представление изучаемого материала в сравнительных или классификационных таблицах, метод опорных схем.

Тема 4. «Основы противодействия киберпреступности». Рассказ, объяснение, демонстрация в форме компьютерной презентации, метод опорных схем.

Тема 5. «Компьютерная информация: обнаружение и анализ». Рассказ, объяснение, демонстрация в форме компьютерной презентации, метод опорных схем.

В связи с тем, что обучающимся необходимо не только сформировать знания по учебной дисциплине, но и освоить в полном объеме логические операции анализа и сравнения, одним из востребованных *наглядных методов* проведения лекционных занятий является ***представление изучаемого материала в сравнительных или классификационных таблицах.***

Например, при рассмотрении темы 1 соотношение понятий “защита информации” и “информационная безопасность” рассматриваются в виде сравнительной таблицы:

Защита информации	Информационная безопасность

При рассмотрении темы 2 соотношение понятий «каналы утечки информации» и «методы их обнаружения»:

Каналы утечки информации	Методы их обнаружения

При рассмотрении темы 3 соотношение понятий «методы обеспечения безопасности информации» и «средства обеспечения безопасности информации»:

Методы обеспечения безопасности информации	Средства обеспечения безопасности информации

Среди *визуальных* (*наглядных) методов*, используемых на лекциях по «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» в сочетании с *вербальными* (*словесными)* методами, особо стоит отметить ***метод опорных (структурно-логических) схем,*** которые могут быть воплощены в форме компьютерной презентации или в графической форме.

Цель опорных схем – изложить изучаемый материал так, чтобы на основе логических связей учебного материала он стал более доступным и облегчил запоминание. При этом особую ценность в методическом плане представляет собой опорная схема, воспроизводимая и комментируемая преподавателем в процессе чтения лекции.

При чтении лекции по теме 1 (рис.1), используя блок-схему, характеризующую меры по защите информации, преподаватель раскрывает систему правового регулирования вопросов информатизации и обеспечения информационной безопасности. Поясняет их назначение, раскрывает их содержание.

Также в процессе чтения лекции по теме 1, используя структурную схему методов обеспечения безопасности информации (рис. 2), преподаватель разъясняет обучающимся методы обеспечения безопасности информации.

Следует отметить, что представление изучаемого материала в виде опорных или блок-схем, а также классификационных (сравнительных) таблиц значительно облегчает процесс подготовки обучающихся к практическим занятиям, так как не требует дополнительного поиска учебной информации в различных источниках и систематизирует учебный материал.

Рис. 1. Комплекс мер и мероприятий, направленных на безопасную обработку информации в информационных системах

Рис. 2. Методы обеспечения безопасности информации

Методика проведения семинарских занятий

В соответствии с учебной программой по учебной дисциплине «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» предусмотрено проведение пяти семинарских занятий. Структура семинарских занятий состоит из трех основных элементов: введения, основной части и заключения.

Семинарские занятия по учебной дисциплине развивают профессиональное мышление обучающихся, помогают связывать научно-теоретические положения с практикой и содействуют выработке практических умений и навыков.

Как правило, на семинарском занятии последовательно рассматриваются 4-5 учебных вопросов. При этом перед преподавателем стоят следующие цели:

с одной стороны, необходимо проверить уровень знаний теоретического материала и добиться его безусловного усвоения на минимальном уровне всеми обучающимися;

с другой стороны, на семинарском занятии выносятся для изучения наиболее сложные вопросы, требующие более серьезной проработки.

Проведение семинарского занятия

Вводная часть (до 10 мин)

Занятие начинается с принятия преподавателем доклада командира о готовности учебной группы к занятию и проверке наличия

присутствующих. После доклада преподаватель предлагает обучающимся занять свои места. Затем преподаватель напоминает о требованиях, предъявляемых к обучающимся по ведению конспектов, посещению занятий и консультаций и т. д.

После этого объявляет вид, тему и цели занятия, перечисляет вопросы, которые будут рассматриваться на занятии (по усмотрению преподавателя цели и учебные вопросы могут быть обозначены в завершении вводного слова).

В кратком вводном слове преподаватель показывает актуальность и сложность темы, взаимосвязь с ранее изученными положениями других учебных дисциплин. Преподаватель заканчивает вступительное слово перечислением учебных вопросов, подлежащих рассмотрению (если это не сделано ранее) и определением формы их обсуждения.

Актуализация опорных знаний (по усмотрению преподавателя в зависимости от рассматриваемой темы) по учебной дисциплине заключается в извлечении усвоенного материала из долговременной или кратковременной памяти с целью последующего использования его при узнавании, припоминании, воспоминании или непосредственном воспроизведении. Она проводится любыми из методов на выбор преподавателя: устный опрос (фронтальный, блиц-опрос, опрос по цепочке, опрос в парах, в тройках), письменный опрос, тестирование.

Основная часть

В основной части занятия преподаватель проверяет знания, полученные обучающимися на лекциях и в процессе самостоятельной подготовки по учебным вопросам. Проверка может осуществляться путем блиц-опроса, опроса с ответом перед всей аудиторией (у доски), заслушиванием докладов и др. По усмотрению преподавателя блиц-опрос может проводиться как в начале, так и в конце занятия. Могут заслушиваться доклады, подготовленные обучающимися.

При проведении опроса по учебным вопросам либо заслушивании докладов после каждого выступления преподаватель может обращаться к другим обучающимся с просьбой дополнить предыдущее сообщение либо высказать свое мнение. В зависимости от уровня подготовки обучающегося по учебным вопросам преподаватель уточняет и дополняет ответы самостоятельно либо с помощью обучающихся группы, организует творческую дискуссию, обмен мнениями. Для более успевающих курсантов целесообразно определить роль экспертов, дающих оценку как содержательного уровня ответов обучающихся, так и других его характеристик: знании терминологии, грамотность речи и др. При необходимости преподаватель оказывает помощь в овладении навыками устного изложения материала и ведения полемики. Рассмотрение каждого вопроса (доклада) заканчивается кратким выводом преподавателя.

Для курсантов, успевающих на высоком уровне, целесообразно предусмотреть индивидуальные задания повышенной сложности, предполагающие не только наличие теоретических знаний, но и их применение при решении или анализе конкретных ситуаций.

Для успевающих на низком уровне курсантов целесообразно предусмотреть задания, связанные с воспроизведением в устной или письменной форме теоретического материала после его проработки в составе учебной группы.

При проведении занятия преподаватель обеспечивает активность и работу всей группы. С этой целью обучающимся могут задаваться дополнительные вопросы для их последующего обсуждения, даваться письменные занятия.

Заключительная часть (до 10 мин)

Преподаватель подводит итог, делает объективный анализ и оценивает работу обучающихся на занятии, выявляет положительные стороны и недостатки, анализирует ответы обучающихся и выставляет отметки. В конце занятия преподаватель может оставить 3-5 минут учебного времени для ответов на возможные вопросы обучающихся.

В завершение преподаватель подает объявляет об окончании занятия[2].

Методика проведения практических занятий

В соответствии с учебной программой по учебной дисциплине «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» предусмотрено проведение 14 практических занятий. Структура практических занятий, как правило, состоит из трех основных частей: вводной, основной и заключительной.

Проведение практического занятия.

Вводная часть (до 10 мин)

Преподаватель принимает доклад командира группы, проверяет наличие курсантов и их готовность к занятию (наличие конспектов и т.д.), приводит в готовность технические средства обучения.

Преподаватель объявляет тему практического занятия и ее связи с ранее изученным материалом. Указывает на актуальность и значимость изучаемой темы для практической работы сотрудников органов внутренних дел. Определяет перечень отрабатываемых учебных вопросов, рекомендует необходимую литературу.

Актуализация опорных знаний (по усмотрению преподавателя в зависимости от рассматриваемой темы) по учебной дисциплине заключается в извлечении усвоенного материала из долговременной или кратковременной памяти с целью последующего использования его при

[2] Указанная методика используется при проведении семинарских занятий по всем темам.

узнавании, припоминании, воспоминании или непосредственном воспроизведении. Она проводится любыми из методов на выбор преподавателя: устный опрос (фронтальный, блиц-опрос, опрос по цепочке, опрос в парах, в тройках), письменный опрос, тестирование.

Основная часть.

Выполнение заданий (практическая работа).

Методы: объяснительный; практический.

При необходимости преподаватель, используя свой компьютер и мультимедийную доску демонстрирует приемы и методы решения конкретных практических задач, входящих в круг учебных вопросов практического занятия.

Определяется план выполнения практической части; дается анализ программного обеспечения, технических устройств, тренажёров и т. п., необходимых для выполнения практического задания; объясняется последовательность выполнение прием и операций.

После получения практического задания обучающиеся самостоятельно выполняют его, преподаватель осуществляет контроль за ходом выполнения задания, оказывает помощь, задает вопросы, корректирует работу.

В ходе практического занятия курсантами, как правило, ведется файл-отчет. Файл-отчет сохраняется в виде файла MS Word. Название для файла-отчета формируется по правилу: «номер группы» пробел «фамилия курсанта» пробел «тема занятия» (*например: «0341 Иванов 1.3.5»).* Файлы-отчеты в конце занятия сохраняются в сетевую папку, указанную преподавателем.

При подготовке файла-отчета по каждому заданию данной темы необходимо не только указать конечный результат, но и кратко описать механизм его достижения (*например, структуру поискового запроса либо набор ключевых слов*).

Проверка выполнения задания.

Преподаватель оценивает степень усвоения обучающимися учебных вопросов по результатам выполненных практических заданий. При проверке результатов выполнения практических заданий преподаватель задает уточняющие вопросы, просит обучающегося продемонстрировать приемы выполнения отдельных действий. При наличии времени преподаватель проверяет работы во время занятия (при недостатке времени – после занятия).

Заключительная часть.

Преподаватель совместно со обучающимися обсуждают итоги работы на занятии, дает оценку деятельности обучающихся, отвечает на вопросы курсантов.

Оценка выполнения курсантами практического задания

производится с учетом их ответов на вопросы актуализации опорных знаний, объема выполненного задания. Отметка выставляется в соответствии с принятыми критериями оценки качества знаний и компетенции обучающегося по десятибалльной системе.

Преподаватель называет тему следующего практического занятия, определяет вопросы для подготовки, называет учебную литературу.

3. КРАТКИЕ ДИДАКТИЧЕСКИЕ МАТЕРИАЛЫ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ[3]

Тема 1. Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь

Всего аудиторных –4 часа
Лекции – 2 часа
Семинарские – 2 часа

Вопросы лекции:

1. Понятие, содержание информационной безопасности.
2. Правовое обеспечение информационной безопасности.
3. Основные направления обеспечения информационной безопасности.

Вопросы семинарского занятия:

1. Правовое и организационно-техническое обеспечение информационной безопасности.
2. Меры по обеспечению информационной безопасности.
3. Государственные органы, обеспечивающие информационную безопасность в Республике Беларусь.
4. Место Министерства внутренних дел в системе государственных органов, обеспечивающих информационную безопасность в Республике Беларусь.

Вопросы для самоконтроля и актуализации знаний:

1. Технические требования, предъявляемые к защищенным компьютерным системам.
2. Каналы утечки информации и методы их обнаружения.
3. Методы и средства защиты информации в компьютерных системах от разведывательной деятельности, шпионажа и диверсий.

Литература: 1, 3, 5, 6, 9, 11, 12, 13, 20

Тема 2. Каналы утечки информации и безопасность информационных систем

[3] Дидактические материалы для проведения практических занятий в полном объеме хранятся в электронном виде в сетевой папке \\fs10\курсант\ПКПиОЗИ.

Всего аудиторных – 4 часа
Лекции – 2 часа
Семинарские – 2 часа

Вопросы лекции:

1. Основные угрозы безопасности информационных систем.
2. Каналы утечки информации: виды, содержание, особенности реализации.
3. Способы и средства предотвращения утечки информации.

Вопросы семинарского занятия:

1. Угрозы информационной безопасности и их источники. Неформальная модель возможного нарушителя информационной безопасности.
2. Каналы утечки информации: виды, содержание, особенности реализации.
3. Способы обнаружения (выявления) технических каналов утечки информации.
4. Защита информации ограниченного распространения от утечки через технические каналы утечки информации.
5. Основные подходы к защите информации в Едином цифровом пространстве МВД Республики Беларусь.

Вопросы для самоконтроля и актуализации знаний:

1. Основные угрозы безопасности информационных систем: понятия, классификация, механизм реализации.
2. Виды, содержание, особенности реализации каналов утечки информации.
3. Раскройте особенности предотвращения утечки информации.

Литература: 1, 4, 5, 6, 7, 12, 15, 22

Тема 3. Аппаратное и программное обеспечение защищенных компьютерных систем

Всего аудиторных – 18 часов
Лекции – 2 часа
Семинарские – 2 часа
Практические – 14 часов

Вопросы лекции:

1. Операционные системы и их защищенность.

2. Методы и средства защиты информации в компьютерных системах.

Вопросы семинарского занятия:

1. Политика информационной безопасности единой цифровой платформы Министерства внутренних дел Республики Беларусь.
2. Особенности фундаментального подхода к построению архитектуры системы защиты. Подсистемы безопасности операционной системы.
3. Криптографическая защита данных. Виртуальные частные сети (VPN).
4. Контроль целостности и аутентичности (подлинности и авторства) данных, передаваемых по каналам связи. Электронная цифровая подпись.
5. Защита периметра компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы). Обнаружение атак (опасных действий нарушителей) и оперативное реагирование.

Вопросы практического занятия 3.3:

1. Настройка параметров доверенной загрузки операционной системы.
2. Аутентификация, авторизация и управление доступом в ОС Windows.
3. Политики безопасности ОС.
4. Регистрация и оперативное оповещение о событиях безопасности.

Вопросы практического занятия 3.4:

1. Антивирусное программное обеспечение.
2. Межсетевое экранирование.
3. Изолированная среда исполнения с контролируемыми правами.
4. Резервное копирование. Создание образа системы.

Вопросы практического занятия 3.5:

1. Шифрование файлов и папок пользователя с использованием файловой системы EFS.
2. Создание и использование электронной цифровой подписи средствами операционной системы.

Вопросы практического занятия 3.6:

1. Шифрование данных средствами прикладных программных продуктов.

2. Создание и использование защищенных криптоконтейнеров TrueCrypt.

3. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force.

4. Стеганографические методы защиты информации.

Вопросы практического занятия 3.7:

1. Средства виртуализации: установка, настройка и использование.

2. Гостевая ОС Linux: установка и администрирование. Онлайн-определение параметров User Agent.

Вопросы практического занятия 3.8:

1. Методы восстановления удаленной информации с электронных носителей с использованием специального программного обеспечения.

2. Порядок удаления информации программными способами без возможности ее восстановления.

3. Проверка и удаление следов активности пользователя в системе.

Вопросы практического занятия 3.9:

1. Организация безопасного хранения паролей в защищаемых компьютерных системах.

2. Защита файлов и папок от несанкционированного доступа.

3. Защита съемных носителей информации от несанкционированного доступа. Блокировка записи на USB-носители.

Вопросы для самоконтроля и актуализации знаний:

1. Что такое аутентификация и идентификация? Для чего применяются эти механизмы?

2. Что такое учётная запись пользователя? Какие средства аутентификации могут быть использованы для повышения надёжности защиты учетной записи компьютера?

3. Аудит системы безопасности. Журнал событий.

4. Что такое виртуальная машина? Где она может использоваться?

5. В чем заключается основной алгоритм работы программ восстановления удаленной информации?

6. Что представляет собой безвозвратное уничтожение данных? На чем основаны существующие программные реализации алгоритмов безвозвратного уничтожения данных?

7. Что такое шифрование? Что такое «прозрачное шифрование»?

8. Перечислите и охарактеризуйте функциональные особенности системы шифрования EFS.

9. Что означает двухуровневая парольная защита смонтированного с помощью «TrueCrypt» тома?

10. Что такое стеганография? Для чего она применяется?

Литература: 1, 4, 5, 7, 8, 9, 10, 12, 15, 22

Тема 4. Основы противодействия киберпреступности

Всего аудиторных – 8 часов
Лекции – 2 часа
Семинарские – 2 часа
Практические – 4 часа

Вопросы лекции:

1. Киберпреступность: сущность и содержание, особенности противодействия.
2. Глобальная сеть Интернет как среда совершения киберпреступлений.
3. Особенности получения информации из открытых источников сети Интернет для решения служебных задач.

Вопросы семинарского занятия:

1. Классификация преступлений, совершаемых с использованием информационно-коммуникационных технологий.
2. Способы совершения киберпреступлений и особенности правоприменительной практики.
3. Значение сетевой адресации (IP, MAC, DNS) в противодействии киберпреступности.
4. Особенности поиска оперативно-значимой информации из открытых источников сети Интернет, социальных сетей и DarkNet.

Вопросы практического занятия 4.3:

1. Сетевой IP-адрес, символьный (DNS) и MAC-адрес сетевого адаптера или порта маршрутизатора.
2. Способы установления IP-адреса и сведений о нем. Возможности установления личности по IP и MAC–адресам.
3. Использование виртуальных частных сетей (VPN) и прокси-серверов (анонимайзеров) в ходе веб-серфинга.
4. Составление запросов операторам электросвязи на получение информации.

Вопросы практического занятия 4.4:

1. Поиск информации в сети Интернет для решения задачи противодействия преступности.

2. Проверка адреса электронной почты (E-mail) и связанных с ним аккаунтов на предмет возможной компрометации.

3. Установление сведений о банковской платежной карточке (вид платежной системы, банк-эмитент, тип и статус карты) по банковскому идентификационному номеру BIN.

Вопросы для самоконтроля и актуализации знаний:

1. Что такое IP-адрес? Из каких составных частей он состоит? Особенности TCP/IP адресации. Статический и динамический IP-адрес.

2. Является ли знание IP адреса средства компьютерной техники достаточным для его однозначной идентификации?

3. Доменные имена. Группы доменов. Использование доменов.

4. Перечислите и охарактеризуйте операторы поискового контекста и документные операторы системы «Яндекс».

5. Операторы поисковой системы «Google». Расширенный поиск «Google».

6. Специализированный поиск людей в «Яндекс».

7. Установление факта редактирования цифрового изображения.

8. Визуализация связей в социальных сетях.

9. Поиск сохраненных (кэшированных) копий веб-страниц.

Литература: 2, 4, 5, 7, 11, 12, 15, 19, 20, 22

Тема 5. Компьютерная информация: обнаружение и анализ

Всего аудиторных – 12 часов
Лекции – 2 часа
Семинарские – 2 часа
Практические – 10 часов

Вопросы лекции:

1. Средства компьютерной техники (далее – СКТ) как источники компьютерной информации.

2. Особенности осмотра СКТ и компьютерной информации: программно-технические аспекты.

3. Особенности осмотра удаленных ресурсов и электронной почты: программно-технические аспекты.

Вопросы семинарского занятия:

1. Понятие компьютерной информации.

2. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на компьютере, находящемся во включенном состоянии.

3. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на компьютере, находящемся в выключенном состоянии.

4. Особенности исследования и использования компьютерной информации, содержащей электронно-цифровые следы.

5. Программно-техническое обеспечение осмотра и анализа СКТ.

Вопросы практического занятия 5.3:

1. Анализ СКТ (электронных носителей информации) средствами операционной системы.

2. Анализ системных файлов, файлов реестра, хронологии событий операционной системы.

Вопросы практического занятия 5.4:

1. Изучение функционального назначения прикладного программного обеспечения «НИРСОФТ».

2. Анализ СКТ с использованием прикладного программного обеспечения «НИРСОФТ».

Вопросы практического занятия 5.5:

1. Изучение структуры и содержания информации, извлеченной из исследуемых СКТ.

2. Анализ информации, извлеченной из исследуемых СКТ (на примере программно-технического комплекса «Мобильный криминалист»).

Вопросы практического занятия 5.6:

1. Изучение структуры и содержания логических и физических образов, извлеченных из исследуемых мобильных устройств.

2. Анализ информации, извлеченной из мобильных устройств (на примере программно-технического комплекса «Мобильный криминалист»)

Вопросы практического занятия 5.7:

1. Осмотр компьютерной информации (программно-технические аспекты):

интернет-ресурс;

электронная почта (E-mail).

Вопросы для самоконтроля и актуализации знаний:

1. Особенности осмотров с участием специалиста.
2. Особенности поиска и изъятия информации и следов воздействия на нее.
3. Специфические особенности осмотра удаленных ресурсов и трафика.
4. Процессуальный и технический порядок оформления результатов осмотра.
5. Подготовительный этап проведения осмотра компьютерной техники.
6. Содержание протокола осмотра компьютерной техники. Особенности оформления протокола осмотра средств компьютерной техники.
7. Меры по обеспечению сохранности исследуемой компьютерной информации и служебного компьютерного обеспечения при проведении осмотров изъятых машинных носителей
8. Перечень программного обеспечения, которое должно быть установлено на служебных компьютерных средствах для проведения исследования машинных носителей.
9. Опишите механизм составления постановления о назначении компьютерно-технической экспертизы. Перечислите вопросы эксперту.

Литература: 2, 4, 5, 7, 12, 13, 14, 15, 19, 20, 22

4. МЕТОДИКА ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа (СР) – это деятельность обучающегося, направленная на самостоятельное овладение обучающимися частью содержания изучаемой дисциплины при помощи специально разработанного научно-методического обеспечения и предполагающая организацию дополнительных консультаций и специальных видов контроля со стороны преподавателя, помимо предусмотренных учебным планом форм промежуточного и итогового контроля компетенций обучающихся по изучаемой дисциплине.

СР, как важная часть образовательного процесса, способствует мотивации обучающихся, должна сопровождаться доступным и качественным научно-методическим и материально-техническим обеспечением, эффективной системой контроля и содействовать усилению практической направленности обучения.

Целями СР являются:

создание условий для реализации творческих способностей обучающихся, развития их академических, профессиональных, социально-личностных компетенций, активного включения в учебную, научную, общественную и инновационную деятельность;

реализация принципов инновационного образования в учебной и научно-методической работе профессорско-преподавательского состава;

саморазвитие и творческая самореализация обучающихся.

Важнейшими задачами СР выступают:

активизация роли обучающихся в самостоятельном получении знаний и применении их на практике;

содействие выстраиванию каждым обучающимся собственной образовательной траектории в рамках самостоятельной работы.

Научно-методическое обеспечение СР по учебной дисциплине включает обязательную и вариативную части.

Обязательная часть научно-методического обеспечения СР по учебной дисциплине включает:

теоретический материал и перечень основной литературы, необходимые для выполнения СР;

перечни заданий и контрольных мероприятий СР;

фонды оценочных средств: типовые задания, открытые задания, тесты, алгоритмы выполнения заданий, примеры решения задач, тестовые задания для самопроверки и самоконтроля, тематика рефератов..

Вариативная часть научно-методического обеспечения СР по учебной дисциплине включает: наглядные пособия, мультимедийные, аудио- и видеоматериалы, электронные информационные ресурсы (локальный доступ, удаленный доступ) и др.

СР проводится за счет аудиторных часов (лекционных, семинарских

и практических), предусмотренных учебными планами на изучение учебной дисциплины.

Преподаватель на первом занятии информирует обучающихся о методике организации и проведения СР. Для методической поддержки СР могут проводиться дополнительные консультации.

Формами СР являются: выполнение исследовательских и творческих заданий: подготовка сообщений, тематических докладов, рефератов, презентаций, эссе; выполнение практических заданий, решение задач, составление алгоритмов, схем,; аналитическая обработка текста (аннотирование, рецензирование, составление резюме, конспектирование); разбор кейсов; создание «портфолио»; выполнение проектов; оформление рекламных, информационных и демонстрационных материалов (стенды, газеты и пр.); составление тестов; изготовление макетов; составление тематической подборки литературных источников, интернет-источников; оформление и сопровождение ингернет-страниц, сайтов, блогов; выполнение открытых заданий и др.

Задания для СР должны учитывать индивидуальные особенности обучающихся и быть дифференцированы по уровням сложности.

5. МЕТОДИКА КОНТРОЛЯ И ОЦЕНКИ ЗНАНИЙ

Результаты текущего контроля знаний отражаются преподавателем в журнале учета учебных занятий. Десятибалльная шкала оценки представляет собой систему измерения учебных достижений обучающихся, в которой отметка уровня знаний выражается последовательным рядом чисел (баллов) «1», «2», «3», «4», «5», «6», «7», «8», «9», «10». При оценке знаний обучающихся отметками в баллах по десятибалльной шкале учитываются критерии оценки результатов учебной деятельности обучающихся в учреждениях высшего образования по десятибалльной шкале.

Десятибалльная шкала в зависимости от величины балла и отметки включает следующие критерии:

10 (десять) баллов:

систематизированные, глубокие и полные знания по теме занятия, а также по основным вопросам, выходящим за ее пределы;

точное использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы;

безупречное владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач;

выраженная способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации;

полное и глубокое усвоение основной и дополнительной литературы, по изучаемой учебной дисциплине;

умение свободно ориентироваться в теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку, использовать научные достижения других дисциплин;

творческая самостоятельная работа на семинарских и практических, занятиях, активное творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

9 (девять) баллов:

систематизированные, глубокие и полные знания по теме занятия по учебной дисциплине;

точное использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы;

владение инструментарием учебной дисциплины, умение его эффективно использовать в постановке и решении научных и профессиональных задач.

способность самостоятельно и творчески решать сложные проблемы в нестандартной ситуации в рамках учебной дисциплины;

полное усвоение основной и дополнительной литературы, рекомендованной учебной программой по учебной дисциплине;

умение ориентироваться в теориях, концепциях и направлениях по изучаемой теме и давать им аналитическую оценку;

систематическая, активная самостоятельная работа на семинарских и практических, занятиях, творческое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

8 (восемь) баллов:

систематизированные, глубокие и полные знания по теме занятия по учебной дисциплине;

использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения;

владение инструментарием учебной дисциплины (методами комплексного анализа, техникой информационных технологий), умение его использовать в постановке и решении научных и профессиональных задач;

способность самостоятельно решать сложные проблемы в рамках учебной программы по учебной дисциплине;

усвоение основной и дополнительной литературы, рекомендованной учебной программой по учебной дисциплине;

умение ориентироваться в теориях, концепциях и направлениях по изучаемой теме и давать им аналитическую оценку;

активная самостоятельная работа на семинарских и практических, занятиях, систематическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

7 (семь) баллов:

систематизированные, глубокие и полные знания по теме занятия по учебной дисциплине;

использование научной терминологии (в том числе на иностранном языке), грамотное, логически правильное изложение ответа на вопросы, умение делать обоснованные выводы и обобщения;

владение инструментарием учебной дисциплины, умение его использовать в постановке и решении научных и профессиональных задач;

свободное владение типовыми решениями в рамках учебной дисциплины;

усвоение основной и дополнительной литературы, рекомендованной учебной программой по учебной дисциплине;

умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им аналитическую оценку;

самостоятельная работа на семинарских и практических, занятиях, участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

6 (шесть) баллов:

достаточно полные и систематизированные знания по теме занятия по учебной дисциплине;

использование необходимой научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать обобщения и обоснованные выводы;

владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач;

способность самостоятельно применять типовые решения в рамках учебной дисциплины;

усвоение основной литературы, рекомендованной учебной программой по учебной дисциплине;

умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой дисциплине и давать им сравнительную оценку;

активная самостоятельная работа на семинарских и практических, занятиях, периодическое участие в групповых обсуждениях, высокий уровень культуры исполнения заданий.

5 (пять) баллов:

достаточные знания по теме занятия по учебной дисциплине;

использование научной терминологии, грамотное, логически правильное изложение ответа на вопросы, умение делать выводы;

владение инструментарием учебной дисциплины, умение его использовать в решении учебных и профессиональных задач;

способность самостоятельно применять типовые решения в рамках учебной дисциплины;

усвоение основной литературы, рекомендованной учебной программой по учебной дисциплине;

умение ориентироваться в базовых теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им сравнительную оценку;

самостоятельная работа на семинарских и практических, занятиях, фрагментарное участие в групповых обсуждениях, достаточный уровень культуры исполнения заданий.

4 (четыре) балла:

достаточный объем знаний в рамках образовательного стандарта высшего образования;

усвоение основной литературы, рекомендованной учебной программой по учебной дисциплине;

использование научной терминологии, логическое изложение ответа на вопросы, умение делать выводы без существенных ошибок;

владение инструментарием учебной дисциплины, умение его использовать в решении стандартных (типовых) задач;

умение под руководством преподавателя решать стандартные (типовые) задачи;

умение ориентироваться в основных теориях, концепциях и направлениях по изучаемой учебной дисциплине и давать им оценку;

работа под руководством преподавателя на семинарских и практических, занятиях, допустимый уровень культуры исполнения заданий.

3 (три) балла:

недостаточно полный объем знаний в рамках образовательного стандарта высшего образования;

знание части основной литературы, рекомендованной учебной программой по учебной дисциплине;

использование научной терминологии, изложение ответа на вопросы с существенными, логическими ошибками;

слабое владение инструментарием учебной дисциплины, некомпетентность в решении стандартных (типовых) задач;

неумение ориентироваться в основных теориях, концепциях и направлениях изучаемой учебной дисциплины;

пассивность на семинарских и практических занятиях, низкий уровень культуры исполнения заданий.

2 (два) балла:

фрагментарные знания в рамках образовательного стандарта высшего образования;

знания отдельных литературных источников, рекомендованных учебной программой учреждения высшего образования по учебной дисциплине;

неумение использовать научную терминологию учебной дисциплины, наличие в ответе грубых, логических ошибок;

пассивность на семинарских и практических занятиях, низкий уровень культуры исполнения заданий.

1 (один) балл:

отсутствие знаний и (компетенций) в рамках образовательного стандарта высшего образования, отказ от ответа.

Положительными являются отметки не ниже 4 (четырех) баллов. Отметки 1 (один), 2 (два), 3 (три) балла являются неудовлетворительными. Результаты текущего контроля знаний отражаются преподавателем в журнале учета учебных занятий.

Отработка обучающимися неудовлетворительных отметок осуществляется по решению кафедры или преподавателя, ведущего занятия в учебной группе. Отметка по результатам отработки выставляется в журнале учета учебных занятий через дробь.

Промежуточная аттестация по учебной дисциплине «Комплексная защита информации и противодействие киберпреступности» проводится в форме зачета по билетам, разработанным кафедрой.

Основная литература

1. Организация работы в защищенных компьютерных системах : учебно-методическое пособие / П. Л. Боровик, А. П. Жалов ; Учреждение образования "Академия Министерства внутренних дел Республики Беларусь". – Минск : Академия МВД, 2018. – 154 с.

2. Лахтиков, Д. Н. Компьютерные термины, сленг, жаргон, сокращения : пособие / Д. Н. Лахтиков ; учреждение образования «Акад. М-ва внутр. Дел Респ. Беларусь». – Минск : Академия МВД, 2022. – 71 с.

3. Лахтиков, Д. Н. Противодействие мошенничеству с использованием электронных средств платежа : учебно-практическое пособие / Д. Н. Лахтиков, П. Л. Боровик; под ред. Н. В. Голубых. – Екатеринбург: Уральский юридический институт МВД России, 2022. – Гл. 2. – С. 19–60.

Дополнительная литература

4. 4. Организация расследования преступлений в сфере высоких технологий : учебное пособие / П. В. Гридюшко[и др.]; под общ.ред. И. Г. Мухина ; Учреждение образования "Академия Министерства внутренних дел Республики Беларусь". – Минск : Академия МВД, 2016. – 154 с.

5. Лепехин, А.Н. Основы информационной безопасности: практикум / А. Н. Лепехин, П.Л. Боровик; М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск: Акад. МВД, 2013. – 80 с.

Нормативные правовые акты[4]

6. Инструкция о порядке использования ведомственной сети передачи данных и глобальной компьютерной сети Интернет в органах внутренних дел и внутренних войсках Министерства внутренних дел Республики Беларусь: Приказ МВД Республики Беларусь, 19 сентября 2017 г., № 267.

7. Концепция национальной безопасности Республики Беларусь : Указ Президента Республики Беларусь 9 ноября 2010 г., № 575 // Консультант Плюс : Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой информации Республики Беларусь. – Минск, 2023.

8. О единой цифровой платформе Министерства внутренних дел : приказ М-ва внутр. дел Респ. Беларусь от 30 сентября 2022 г., № 256.

9. О кибербезопасности: утв. Указом Президента Республики Беларусь 14 февр. 2023 г., № 40 // Консультант Плюс : Беларусь.

[4] Нормативные правовые акты используются в действующей редакции на момент изучения учебной дисциплины

[Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой информации Республики Беларусь. – Минск, 2023.

10. О концепции информационной безопасности Республики Беларусь : постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., №1 // Консультант Плюс: Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой информации Республики Беларусь. – Минск, 2023.

11. О мерах по совершенствованию использования национального сегмента сети Интернет: утв. Указом Президента Республики Беларусь 1 февр. 2010 г., № 60 // Консультант Плюс : Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой информации Республики Беларусь. – Минск, 2023.

12. Об информации, информатизации и защите информации : Закон Республики Беларусь, 10 ноября 2008 г., №455-З // Консультант Плюс : Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой информации Республики Беларусь. – Минск, 2023.

6. Об утверждении Инструкции об организации технической защиты информации, не отнесенной к государственным секретам, в государственных информационных системах органов внутренних дел и внутренних войск Министерства внутренних дел Республики Беларусь : Приказ МВД Республики Беларусь, 19 декабря 2019 г. № 331.