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
31.10.2023

Регистрационный № 2/19-76

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

по изучению 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

Минск, 2023

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 учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № ___ от _____ 2023 г.)

ВВЕДЕНИЕ

Учебная дисциплина «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» предназначена для специальностей 6-05-0421-01 (1-24 01 02) Правоведение, 6-05-0421-03 (1-24 01 03) Экономическое право.

Целями изучения учебной дисциплины «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» являются 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.

Основными задачами изучения учебной дисциплины «Комплексная защита информации и противодействие киберпреступности» 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.

Методика подготовки и работы на лекционном занятии по учебной дисциплине

В соответствии с учебной программой по учебной дисциплине «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» для дневной формы получения образования предусмотрено проведение пяти лекционных занятий.

При подготовке к лекционным занятиям курсантам необходимо:

изучить вопросы к лекции;

ознакомиться со списком литературой по теме лекции.

Лекция требует работы обучающегося, чтобы зафиксировать основные этапы развития мысли, выводы-обобщения.

Запись лекции должна начинаться с четкого формулирования темы и плана лекции. Конспектируются основные понятия, определения и выводы, и иной материал по усмотрению обучающегося.

После лекции, с целью закрепления и углубления знаний, обучающиеся должны самостоятельно, с помощью предлагаемой в методических рекомендациях литературы, углубить знания по изучаемой теме.

Методика подготовки к практическим и семинарским занятиям по учебной дисциплине.

Практические и семинарские занятия имеют большое значение в образовательном процессе. Курсанты учатся самостоятельно выполнять практические и ситуационные задания, приобретают умения и навыки работы с информационными технологиями для решения профессиональных задач, углубляют теоретические знания.

При подготовке к практическим и семинарским занятиям необходимо:

повторить материал, пройденный на лекционных занятиях;

изучить вопросы, подлежащие рассмотрению на семинарском занятии;

рассмотреть вопросы, вынесенные на самостоятельную подготовку;

ознакомиться с практическим заданием;

изучить предлагаемую литературу.

Подготовка к семинарскому и практическому занятию и его выполнение должны найти свое отражение в записях в конспекте.

В случае отсутствия на практическом занятии курсант должен выполнить практическое задание и предъявить его преподавателю в согласованное с ним время.

Преподаватель может предложить отдельным курсантам в силу их более глубокой по сравнению с другими обучающимися подготовки индивидуальные задания для усвоения материала.

К промежуточной аттестации допускаются обучающиеся, сдавшие все предусмотренные учебной программой формы промежуточного контроля знаний.

В учебно-методическом кабинете кафедры информационного права факультета криминальной милиции имеются материалы лекций, практические задания, тестовые задания, отражающие все положения изучаемой учебной дисциплины.

В системе контроля используются:

текущая проверка и оценка знаний, проводимая в ходе повседневных учебных занятий;

проверка и оценка знаний на промежуточной аттестации.

Основная литература включает минимум источников, который необходим обучающимся для формирования понятийного аппарата учебной дисциплины, полного и твердого освоения учебного материала.

Дополнительная литература рекомендуется для более углубленного изучения программного материала, расширения кругозора обучающихся, написания рефератов, докладов и научных работ.

СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

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.

Основные понятия и ключевые определения, которые должны быть законспектированы.

Понятие и содержание информационной безопасности в системе национальной безопасности Республики Беларусь. Нормативные правовые акты, регулирующие обеспечение информационной безопасности в Республике Беларусь. Организационные и технические меры, направленные на обеспечение информационной безопасности. Государственные органы, обеспечивающие информационную безопасность в Республике Беларусь. Роль органов внутренних дел в системе государственных органов, обеспечивающих информационную безопасность в Республике Беларусь..

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

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.

Основные понятия и ключевые определения, которые должны быть законспектированы.

Понятие и содержание основных категорий в сфере защиты информации, обрабатываемой в информационных системах. Свойства защищенности информации. Угрозы безопасности и методы их осуществления.

Каналы утечки информации: виды, содержание, особенности реализации.

Способы обнаружения (выявления) технических каналов утечки информации. Защита информации ограниченного распространения от утечки через технические каналы 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.

Основные понятия и ключевые определения, которые должны быть законспектированы.

Операционные системы и их защищенность. Особенности фундаментального подхода к построению архитектуры системы защиты.

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.

Основные понятия и ключевые определения, которые должны быть законспектированы.

Современные подходы к определению понятия и содержанию киберпреступности. Особенности предупреждения киберпреступлений. Глобальная компьютерная сеть Интернет: структура, основные понятия и термины, необходимые в работе сотрудника ОВД (ДФР). Основы поисковой деятельности в сети Интернет: использование поисковых ресурсов; использование иных информационных систем

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.

Основные понятия и ключевые определения, которые должны быть законспектированы.

Понятие компьютерной информации и ее классификация.

Цифровые идентификаторы и их характеристика.

Обнаружение и анализ компьютерной информации.

Средства компьютерной техники как источник компьютерной информации. Особенности осмотра средств компьютерной техники и компьютерной информации: программно-технические аспекты. Особенности исследования компьютерной информации. Особенности осмотра удаленных ресурсов.

Современные программно-аппаратные средства исследования и анализа компьютерной информации.

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

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[1]

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. [Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой

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

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.