Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

УТВЕРЖДАЮ
Первый заместитель
начальника учреждения
образования «Академия
Министерства внутренних дел
Республики Беларусь»
полковник милиции
А.В.Башан
21.04.2023

Регистрационный № УД-331-23-1/уч

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ И ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ (ПКиОЗИ)
МОДУЛЬ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
Учебная программа учреждения высшего образования
по учебной дисциплине для специальностей:
6-05-0421-01 (1-24 01 02) Правоведение
6-05-0421-03 (1-24 01 03) Экономическое право

2023

Учебная программа составлена на основе образовательных стандартов общего высшего образования по специальностям 1-24 01 02 «Правоведение», 1-24 01 03 Экономическое право, утвержденного постановлением Министерства образования Республики Беларусь от 07.07.2022 г. № 180, учебных планов учреждения образования «Академия Министерства внутренних дел Республики Беларусь» по специальностям 1-24 01 02 «Правоведение», 1-24 01 03 «Экономическое право», квалификационной характеристики специалиста-выпускника по специальностям: 1-24 01 02 «Правоведение», 1-24 01 03 «Экономическое право».

Начиная с набора 2023года

Учебная программа составлена на основе проектов образовательных стандартов общего высшего образования по специальностям 6-05-0421-01 «Правоведение», 6-05-0421-03 «Экономическое право», примерных учебных планов по специальности 6-05-0421-01 «Правоведение» от 30.01.2023 № 6-05-04-016/пр., по специальности 6-05-0421-03 «Экономическое право» от 30.01.2023 № 6-05-04-017/пр.; учебных планов учреждения образования «Академия Министерства внутренних дел Республики Беларусь» по специальностям: 6-05-0421-01 «Правоведение», 6-05-0421-03 «Экономическое право»; квалификационных характеристик специалиста-выпускника по специальностям «Правоведение», «Экономическое право».

СОСТАВИТЕЛЬ:

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

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой информационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 9 от 28.03.2023).

Начальник кафедры
информационного права факультета
криминальной милиции
полковник милиции

Д.Н.Лахтиков

. .2023

Научно-методическим советом учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 19 от 07.06.2023).

Оформление учебной программы и сопровождающих ее материалов действующим требованиям Министерства образования Республики Беларусь соответствует.

Эксперт – начальник
учебно-методического управления
полковник милиции

Е.В.Котенко

. .2023

СОГЛАСОВАНО
Письмо центрального аппарата
Следственного комитета
Республики Беларусь

от . .2023 № _____

СОГЛАСОВАНО
Письмо Государственного
пограничного комитета
Республики Беларусь

от . . 2023 №_____

СОГЛАСОВАНО
Письмо
Департамента финансовых
расследований Комитета
государственного контроля
Республики Беларусь

от . . 2023 №_____

СОГЛАСОВАНО
Письмо
Министерства обороны
Республики Беларусь

от . . 2023 №___

СОГЛАСОВАНО
Письмо Департамента
исполнения наказаний
МВД Республики Беларусь

от . . 2023 №____

СОГЛАСОВАНО
Письмо главного управления
уголовного розыска
криминальной милиции
МВД Республики Беларусь

от . . 2023 №_____

СОГЛАСОВАНО
Письмо главного управления
по противодействию
киберпреступности
криминальной милиции
МВД Республики Беларусь

от . . 2023 №

СОГЛАСОВАНО
Письмо главного управления по
наркоконтролю и
противодействию торговле
людьми криминальной милиции
МВД Республики Беларусь

от . . 2023 №

СОГЛАСОВАНО
Письмо главного управления
по борьбе с экономическими
преступлениями
криминальной милиции
МВД Республики Беларусь

от . . 2023 №_____

СОГЛАСОВАНО
Письмо главного управления
охраны правопорядка и
профилактики милиции
общественной безопасности
МВД Республики Беларусь

от . . 2023 №_____

СОГЛАСОВАНО
Письмо управления
надзорно-исполнительной
деятельности
МВД Республики Беларусь

СОГЛАСОВАНО
Письмо главного управления
Государственной автомобильной
инспекции милиции
общественной безопасности
МВД Республики Беларусь

от . . 2023 №_____

СОГЛАСОВАНО
Начальник факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
полковник милиции
А.В.Малахов
. .2023

СОГЛАСОВАНО
Начальник уголовно-исполнительного факультета учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
полковник милиции
О.М.Савастей
. .2023

СОГЛАСОВАНО
Начальник факультета повышения квалификации и переподготовки руководящих кадров учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
полковник милиции
И.В.Ломоть
. .2023

от . . 2023 №____

СОГЛАСОВАНО
Декан факультета права учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
А.В.Долидович
. .2023

СОГЛАСОВАНО
Начальник факультета милиции общественной безопасности учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
полковник милиции
В.М.Коношенко
. .2023

СОГЛАСОВАНО
Начальник следственно-экспертного факультета учреждения образования «Академия Министерства внутренних дел Республики Беларусь»
полковник милиции
Р.В.Скачек
. .2023

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Цели и задачи учебной дисциплины

Учебная программа по учебной дисциплине «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 «Противодействие киберпреступности и основы защиты информации (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.

Место учебной дисциплины в системе подготовки специалиста с высшим образованием, связи с другими учебными дисциплинами

Учебная дисциплина «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» содержится в компоненте учреждения высшего образования учебных планов учреждения образования «Академия Министерства внутренних дел Республики Беларусь» в модуле «Информационная безопасность» по специальностям 6-05-0421-01 (1-24 01 02) «Правоведение» и 6-05-0421-03 (1-24 01 03) «Экономическое право».

Для усвоения содержания учебной дисциплины «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» модуля «Информационная безопасность» необходимо знание основных положений учебных дисциплин «Практикум по информационным технологиям», «Информационное обеспечение служебной деятельности», «Уголовное право», «Уголовный процесс», «Криминалистика».

Требования к освоению учебной дисциплины

Учебная дисциплина «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» направлена на формирование следующих компетенций:

Учебная дисциплина «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» направлена на формирование следующих компетенций для специальностей:

6-05-0421-01 (1-24 01 02) *«Правоведение»:* СК-18 – Владеть технологиями применения информационных ресурсов, программных и аппаратных средств, используемых в решении профессиональных задач в сфере защиты информации и противодействия киберпреступности; СК-17 – Владеть технологиями применения информационных ресурсов, программных и аппаратных средств, используемых в решении профессиональных задач в сфере защиты информации и противодействия киберпреступности;

6-05-0421-03 (1-24 01 03) *«Экономическое право»:* СК-15 – Владеть технологиями применения информационных ресурсов, программных и аппаратных средств, используемых в решении профессиональных задач в сфере защиты информации и противодействия киберпреступности; СК-17 – Владеть технологиями применения информационных ресурсов, программных и аппаратных средств, используемых в решении профессиональных задач в сфере защиты информации и противодействия киберпреступности.

В результате изучения учебной дисциплины «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» обучающийся должен:

знать:

понятие, содержание, направления и особенности правового регулирование обеспечения информационной безопасности;

понятие, виды и каналов утечки информации;

методы и средства обеспечения информационной безопасности;

понятие, сущность и классификации киберпреступлений;

особенности обнаружения и анализа компьютерной информации при противодействии киберпреступности;

уметь:

применять программное обеспечение, используемое для защиты информации;

применять программное обеспечение, используемое для восстановления информации;

осуществлять поиск информации в сети Интернет;

осматривать компьютерную информацию;

владеть:

современными средствами телекоммуникаций;

навыками обнаружения компьютерной информации, содержащей электронно-цифровые следы преступнойдеятельности.

Общее количество часов и количество аудиторных часов, отводимое на изучение учебной дисциплины в соответствии с учебным планом учреждения высшего образования по специальности

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 – 3.

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

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:

9 семестр (5 семестр – с набора 2022 года): общее количество часов – 49 часов, количество аудиторных часов – 2, из которых 2 часа – лекции.

10 семестр (6 семестр – с набора 2022 года): общее количество часов – 49 часов, количество аудиторных часов – 10, из которых 2 часа – лекции, 8 часов – практические занятия.

Форма промежуточной аттестации по учебной дисциплине: экзамен в 10 (6 семестр – с набора 2022 года) 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.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

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

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.

Тема 2. Каналы утечки информации и безопасность информационных систем

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 от утечки через технические каналы утечки информации.

Тема 3. Аппаратное и программное обеспечение защищенных компьютерных систем

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

Методы и средства защиты информации в компьютерных системах.

Тема 4. Основы противодействия киберпреступности

Современные подходы к определению понятия и содержанию киберпреступности. Глобальная компьютерная сеть Интернет: структура, основные понятия и термины, необходимые в работе сотрудника правоохранительных органов. Основы поисковой деятельности в сети Интернет: использование поисковых ресурсов; использование иных информационных систем.

Тема 5. Компьютерная информация: обнаружение и анализ

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.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА 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
дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
7 семестр					
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**	**2**		
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2			
1.2	1. Правовое обеспечение информационной безопасности. 2. Меры по обеспечению информационной безопасности. 3. Государственные органы, обеспечивающие информационную безопасность в Республике Беларусь. 4. Роль Министерства внутренних дел в системе государственных органов, обеспечивающих информационную безопасность в Республике Беларусь.		2		Устный опрос
Тема 2	**Каналы утечки информации и безопасность информационных систем**	**2**	**2**		
2.1	1. Основные угрозы безопасности информационных систем. 2. Каналы утечки информации: виды, содержание, особенности реализации. 3. Способы и средства предотвращения утечки информации.	2			
2.2	1. Угрозы информационной безопасности и их источники. 2. Каналы утечки информации: виды, содержание, особенности реализации. Способы обнаружения (выявления)		2		Устный опрос

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	технических каналов утечки информации. 3. Защита информации от утечки через технические каналы утечки информации. 4. Основные подходы к защите информации в Едином цифровом пространстве МВД Республики Беларусь				
Тема 3	**Аппаратное и программное обеспечение защищенных компьютерных систем**	**2**	**2**	**14**	
3.1	1. Операционные системы и их защищенность. 2. Методы и средства защиты информации в компьютерных системах.	2			
3.2	1. Особенности фундаментального подхода к построению архитектуры системы защиты. Подсистемы безопасности операционной системы. 2. Политика информационной безопасности единой цифровой платформы Министерства внутренних дел Республики Беларусь. 3. Криптографическая защита данных. Виртуальные частные сети (VPN). 4. Защита периметра компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы). Обнаружение атак (опасных действий нарушителей) и оперативное реагирование.		2		Устный опрос
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.			2	Выполнение практических заданий
3.4	1. Антивирусное программное обеспечение. 2. Межсетевое экранирование. 3. Изолированная среда исполнения с контролируемыми правами. 4. Резервное копирование. Создание образа системы.			2	Выполнение практических заданий
3.5	1. Шифрование файлов и папок			2	Выполнение

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	пользователя с использованием файловой системы EFS. 2. Создание и использование электронной цифровой подписи средствами операционной системы.				практических заданий
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.			2	Выполнение практических заданий
3.7	1. Средства виртуализации: установка, настройка и использование. 2. Гостевая ОС Linux: установка и администрирование. Онлайн-определение параметров User Agent.			2	Выполнение практических заданий
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.			2	Выполнение практических заданий
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.			2	Выполнение практических заданий
Тема 4	**Основы противодействия киберпреступности**	**2**	**2**	**4**	
4.1	1. Киберпреступность: сущность и содержание, особенности противодействия. 2. Глобальная сеть Интернет как среда совершения киберпреступлений. 3. Особенности получения информации из открытых источников сети Интернет.	2			
4.2	1. Классификация преступлений,		2		Устный опрос

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	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 информации из открытых источников сети Интернет, социальных сетей и DarkNet.				
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.			2	Выполнение практических заданий
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.			2	Выполнение практических заданий
5	**Компьютерная информация: обнаружение и анализ**	**2**	**2**	**10**	
5.1	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.	2			

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
5.2	1. Компьютерная информация: понятие, виды, идентификаторы. 2. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на СКТ. 3. Особенности обнаружения и анализа компьютерной информации на удаленных ресурсах, в мессенджерах и электронной почте. 4. Программно-техническое обеспечение осмотра и анализа СКТ и компьютерной информации.		2		Устный опрос
5.3	1. Анализ СКТ (электронных носителей информации) средствами операционной системы. 2. Анализ системных файлов, файлов реестра, хронологии событий операционной системы.			2	Выполнение практических заданий
5.4	1. Изучение функционального назначения прикладного программного обеспечения «НИРСОФТ». 2. Анализ СКТ с использованием прикладного программного обеспечения «НИРСОФТ».			2	Выполнение практических заданий
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»).			2	Выполнение практических заданий
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»).			2	Выполнение практических заданий
5.7	1. Осмотр компьютерной информации (программно-технические аспекты): интернет-ресурс;			2	Выполнение практических заданий

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	электронная почта (E-mail).				
	Итого в 7 семестре	**10**	**10**	**28**	
	Форма промежуточной аттестации				**Экзамен**
	Общее количество по учебной дисциплине	**10**	**10**	**28**	**5**

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» для специальности 6-05-0421-01 (1-24 01 02) Правоведение
заочная форма получения высшего образования
срок получения высшего образования 3 года

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	9 семестр (5 семестр – с набора 2021 г.)				
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**			
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2			
	ИТОГО в 9-м семестре (5-м семестр – с набора 2021 г.)	**2**			
	10 семестр (6 семестр – с набора 2021 г.)				
Тема 4	**Основы противодействия киберпреступности**	**2**		**4**	
4.1	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.	2			
4.2	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.			2	Выполнение практических заданий

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
4.3	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.			2	Выполнение практических заданий
5	**Компьютерная информация: обнаружение и анализ**			**4**	
5.1	1. Криминалистический анализ СКТ с использованием прикладного программного обеспечения «НИРСОФТ». 2. Криминалистический анализ информации, извлеченной из мобильных устройств (на примере программно-технического комплекса «Мобильный криминалист»).			2	Выполнение практических заданий
5.2	1. Осмотр компьютерной информации (программно-технические аспекты): интернет-ресурс; электронная почта (E-mail).			2	Выполнение практических заданий
	ИТОГО в 10 семестре (6-м семестре – с набора 2021 г.)	**2**		**8**	
	Форма промежуточной аттестации по учебной дисциплине				**Экзамен**
	Общее количество по учебной дисциплине	**4**		**8**	**3**

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» для специальности 6-05-0421-01 (1-24 01 02) «Правоведение» (профилизации «Судебно-прокурорско-следственная деятельность», «Административно-правовая деятельность») заочная форма получения высшего образования

срок получения высшего образования 5 лет

(для наборов 2021, 2022 годов)

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
9 семестр					
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**			
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2			
Тема 3	**Аппаратное и программное обеспечение защищенных компьютерных систем**			**6**	
3.1	1. Аутентификация, авторизация и управление доступом в ОС Windows. 2. Антивирусное программное обеспечение. 3. Шифрование файлов и папок пользователя с использованием файловой системы EFS.			2	Выполнение практических заданий
3.2	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. Защита съемных носителей информации от несанкционированного доступа. Блокировка записи на USB-носители.			2	Выполнение практических заданий
3.3	1. Методы восстановления удаленной информации с электронных носителей с			2	Выполнение практических

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	использованием специального программного обеспечения. 2. Порядок удаления информации программными способами без возможности ее восстановления. 3. Проверка и удаление следов активности пользователя в системе.				заданий
	ИТОГО в 9 семестре	**2**		**6**	
10 семестр					
Тема 4	**Основы противодействия киберпреступности**			**2**	
4.1	1. Поиск информации в сети Интернет. 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.			2	Выполнение практических заданий
5	**Компьютерная информация: обнаружение и анализ**			**2**	
5.1	1. Анализ СКТ с использованием прикладного программного обеспечения «НИРСОФТ».			2	Выполнение практических заданий
	ИТОГО в 10 семестре			**4**	
	Форма промежуточной аттестации по учебной дисциплине				**Экзамен**
	Общее количество по учебной дисциплине	**2**		**10**	**3**

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» для специальности 6-05-0421-01 (1-24 01 02) «Правоведение» (профилизация «Административно-правовая деятельность») заочная форма получения высшего образования

срок получения высшего образования 5 года (для набора 2020 года)

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
9 семестр					
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**			
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2			
Тема 2	**Каналы утечки информации и безопасность информационных систем**	**2**			
2.1	1. Основные угрозы безопасности информационных систем. 2. Каналы утечки информации: виды, содержание, особенности реализации. 3. Способы и средства предотвращения утечки информации.	2			
Тема 3	**Аппаратное и программное обеспечение защищенных компьютерных систем**	**2**		**4**	
3.1	1. Операционные системы и их защищенность. 2. Методы и средства защиты информации в компьютерных системах.	2			
3.2	1. Аутентификация, авторизация и управление доступом в ОС Windows. 2. Политики безопасности ОС. 3. Антивирусное программное обеспечение.			2	Выполнение практических заданий
3.3	1. Шифрование файлов и папок пользователя с использованием файловой системы EFS. 2. Шифрование данных средствами			2	Выполнение практических заданий

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	прикладных программных продуктов. 3. Методы восстановления удаленной информации с электронных носителей с использованием специального программного обеспечения.				
Тема 4	**Основы противодействия киберпреступности**	**2**			
4.1	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.	2			
	ИТОГО в 9 семестре	**8**		**4**	
10 семестр					
Тема 4	**Основы противодействия киберпреступности**			**2**	
4.1	1. Поиск информации в сети Интернет. 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.			2	Выполнение практических заданий
5	**Компьютерная информация: обнаружение и анализ**			**2**	
5.1	1. Криминалистический анализ СКТ с использованием прикладного программного обеспечения «НИРСОФТ».			2	Выполнение практических заданий
	ИТОГО в 10 семестре			**4**	
	Форма промежуточной аттестации по учебной дисциплине				**Экзамен**
	Общее количество по учебной дисциплине	**8**		**8**	**5**

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

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

2. 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

3. 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.

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.

Нормативные правовые акты[1]

1. 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.

2. 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.

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

4. О кибербезопасности: утв. Указом Президента Республики Беларусь 14 февр. 2023 г., № 40 // Консультант Плюс : Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой информации Республики Беларусь. – Минск, 2023.

5. 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.

6. О мерах по совершенствованию использования национального

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

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.

7. 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.

8. 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.

Методические рекомендации по организации и выполнению самостоятельной работы по учебной дисциплине

Количество учебных часов, отведенных на самостоятельную работу по учебной дисциплине «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» в соответствии с учебным планом Академии МВД для специальностей 6-05-0421-01 (1-24 01 02) Правоведение и 6-05-0421-03 (1-24 01 03) Экономическое право составляет:

дневная форма получения высшего образования – 50 часов;

заочная форма получения высшего образования:
срок получения образования 3 года – 86 часов;

заочная форма получения высшего образования (для профилизаций «Судебно-прокурорско-следственная деятельность», «Административно-правовая деятельность», наборы 2021 и 2022 годов):
срок получения образования 5 лет – 86 часов;

заочная форма получения высшего образования (для профилизации «Административно-правовая деятельность», набор 2020 года):
срок получения образования 5 лет – 128 часов;

Порядок организации самостоятельной работы по учебной дисциплине «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» содержится в методических рекомендациях по изучению учебной дисциплины.

Перечень используемых средств диагностики результатов учебной деятельности

Для диагностики компетенций обучающихся используются следующие устные и письменные формы:

устный опрос;

выполнение практических заданий;

экзамен.

Критерии оценок результатов учебной деятельности.

Для оценки учебных достижений обучающихся используются критерии, рекомендованные Министерством образования Республики Беларусь.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

по учебной дисциплине «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

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Организация и тактика деятельности оперативных подразделений криминальной милиции; Оперативно-розыскная деятельность органов внутренних дел	Оперативно-розыскной деятельности ФКМ	Предложений не поступило	Рекомендовать к утверждению в представленной редакции (протокол № от . . г.)

Начальник кафедры
оперативно-розыскной деятельности
факультета криминальной милиции
полковник милиции А.Н.Тукало

УТВЕРЖДАЮ
Первый заместитель начальника
учреждения образования
«Академия Министерства
внутренних дел
Республики Беларусь»
полковник милиции

А.В.Башан

. .20

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
по учебной дисциплине «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

№№ пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры информационного права факультета криминальной милиции (протокол № ____ от _____ 20 _ г.)

Начальник (заведующий)
кафедры

_____ _____ _____
(ученая степень, ученое звание) (подпись) (И.О.Фамилия)

СОГЛАСОВАНО
_____

_____ _____
(подпись) (И.О.Фамилия)

_____
(дата)

Одобрены и рекомендованы к утверждению научно-методическим советом учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № от 20 года).

УТВЕРЖДАЮ
Первый заместитель начальника
учреждения образования
«Академия Министерства
внутренних дел
Республики Беларусь»
полковник милиции
А.В.Башан
. .2023

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
по учебной дисциплине «Противодействие киберпреступности
и основы защиты информации»
для специальностей 6-05-0421-01/1-24 01 02 Правоведение
6-05-0421-03/1-24 01 03 Экономическое право

№№ пп	Дополнения и изменения	Основание
1.	Абзац 3 оборота титульного листа изложить в новой редакции согласно приложению 1.	Утверждение образовательных стандартов по специальностям 6-05-0421-01 Правоведение 6-05-0421-03 Экономическое право

Учебная программа пересмотрена и одобрена на заседании кафедры и нформационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № от . .2023).

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

Одобрены и рекомендованы к утверждению научно-методическим советом учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № от . .2024).

Приложение 1

Учебная программа составлена на основе образовательных стандартов общего высшего образования по специальностям 6-05-0421-01 «Правоведение», 6-05-0421-03 «Экономическое право», утвержденных постановлением Министерства образования Республики Беларусь от 01.09.2023 г. № 297, примерных учебных планов по специальности 6-05-0421-01 «Правоведение» от 30.01.2023 № 6-05-04-016/пр., по специальности 6-05-0421-03 «Экономическое право» от 30.01.2023 № 6-05-04-017/пр.; учебных планов учреждения образования «Академия Министерства внутренних дел Республики Беларусь» по специальностям: 6-05-0421-01 «Правоведение», 6-05-0421-03 «Экономическое право»; квалификационных характеристик специалиста-выпускника по специальностям «Правоведение», «Экономическое право».

УТВЕРЖДАЮ
Первый заместитель начальника учреждения образования «Академия Министерства внутренних дел Республики Беларусь» полковник милиции

А.В.Башан

29.01.2024

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ

по учебной дисциплине «Противодействие киберпреступности и основы защиты информации (ПКиОЗИ)» модуль «Информационная безопасность» по специальностям 6-05-0421-01 (1-24 01 02) Правоведение, 6-05-0421-03 (1-24 01 03) Экономическое право

№№ п/п	Дополнения и изменения	Основание
1.	Подраздел «Общее количество часов и количество аудиторных часов, отводимое на изучение учебной дисциплины в соответствии с учебным планом учреждения высшего образования по специальности» раздела «Пояснительная записка» для всех форм получения высшего образования дополнить словами: *Дневная форма получения высшего образования:* «Форма текущей аттестации по учебной дисциплине: в 7 семестре – устный опрос по темам 1-5» *Заочная форма получения высшего образования (для наборов 2020 и 2021 годов):* «Форма текущей аттестации по учебной дисциплине: в 10 семестре – устный опрос по темам 1-5» *Заочная форма получения высшего образования (для наборов 2022 и 2023 годов):*	Решение кафедры, протокол № 6 от 27.12.2023.

	«Форма текущей аттестации по учебной дисциплине: в 6 семестре – устный опрос по темам 1-5»	
2.	Учебно-методические карты учебной дисциплины для всех форм получения высшего образования перед пунктом «Форма промежуточной аттестации по учебной дисциплине» дополнить пунктом: «Форма текущей аттестации по учебной дисциплине – устный опрос по темам 1-5»).	

Учебная программа пересмотрена и одобрена на заседании кафедры информационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 6 от 27.12.2023).

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

Одобрены и рекомендованы к утверждению научно-методическим советом учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 6 от 19.01.2024).

УТВЕРЖДАЮ
Начальник учреждения
образования «Академия
Министерства внутренних дел
Республики Беларусь»
генерал-майор милиции
А.П.Васильев
04.07.2024

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
по учебной дисциплине «Противодействие киберпреступности и основы защиты информации» модуль «Информационная безопасность»
по специальностям 6-05-0421-01 (1-24 01 02) Правоведение,
6-05-0421-03 (1-24 01 03) Экономическое право

№№ п/п	Дополнения и изменения	Основание
1.	Тему 4 «Основы противодействия киберпреступности» подраздела «Содержание учебного материала» раздела «Пояснительная записка» дополнить текстом: «Способы совершения киберпреступлений (в т. ч. сопряженные с подменой видео- и (или) аудиоинформации с применением элементов искусственного интеллекта): особенности, порядок обнаружения, анализа и фиксации компьютерной информации, возможности противодействия».	Решение кафедры, протокол № 9 от 29.03.2024
2.	Изложить учебно-методическую карту учебной дисциплины для дневной формы получения высшего образования для специальностей 6-05-0421-01 (1-24 01 02) Правоведение 6-05-0421-03 (1-24 01 03) Экономическое право в новой редакции (приложение 1).	
3.	Изложить раздел «Информационно-методическая часть» в новой редакции (приложение 2).	

Учебная программа пересмотрена и одобрена на заседании кафедры информационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 9 от 29.03.2024).

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

Учреждение образования «Академия Министерства внутренних дел Республики Беларусь»
Рабочий экземпляр № 1

СОГЛАСОВАНО
Начальник факультета
криминальной милиции
полковник милиции
А.В.Говорако
29.03.2024

Одобрены и рекомендованы к утверждению научно-методическим советом учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 12 от 18.06.2024 года).

Приложение 1

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Противодействие киберпреступности и основы защиты информации»
для специальностей 6-05-0421-01 (1-24 01 02) Правоведение
6-05-0421-03 (1-24 01 03) Экономическое право
дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
7 семестр					
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**	**2**		
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2			
1.2	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.		2		Устный опрос
Тема 2	**Каналы утечки информации и безопасность информационных систем**	**2**	**2**		
2.1	1. Основные угрозы безопасности информационных систем. 2. Каналы утечки информации: виды, содержание, особенности реализации. 3. Способы и средства предотвращения утечки информации.	2			
2.2	1. Угрозы информационной безопасности и их источники. Неформальная модель		2		Устный опрос

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	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				
Тема 3	**Аппаратное и программное обеспечение защищенных компьютерных систем**	**2**	**2**	**14**	
3.1	1. Операционные системы и их защищенность. 2. Методы и средства защиты информации в компьютерных системах.	2			
3.2	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. Защита периметра компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы). Обнаружение атак (опасных действий нарушителей) и оперативное реагирование.		2		Устный опрос
3.3	1. Антивирусное программное обеспечение. 2. Резервное копирование. Создание образа системы.			2	Выполнение практических заданий
3.4	1. Шифрование файлов и папок пользователя с использованием файловой системы EFS. 2. Создание и использование электронной цифровой подписи средствами			2	Выполнение практических заданий

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	операционной системы.				
3.5	1. Шифрование данных средствами прикладных программных продуктов. 2. Создание и использование защищенных криптоконтейнеров TrueCrypt.			2	Выполнение практических заданий
3.6	1. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force. 2. Стеганографические методы защиты информации.			2	Выполнение практических заданий
3.7	1. Средства виртуализации: установка, настройка и использование. 2. Гостевая ОС Linux: установка и администрирование. 3. Онлайн-определение параметров User Agent.			2	Выполнение практических заданий
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.			2	Выполнение практических заданий
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.			2	Выполнение практических заданий
Тема 4	**Основы противодействия киберпреступности**	**2**	**2**	**4**	
4.1	1. Киберпреступность: сущность и содержание, особенности противодействия. 2. Способы совершения киберпреступлений (в т. ч. сопряженных с подменой видео- и (или) аудиоинформации с применением элементов искусственного интеллекта). 3. Глобальная сеть Интернет как среда совершения киберпреступлений. 4. Особенности получения информации из	2			

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	открытых источников сети Интернет для решения служебных задач.				
4.2	1. Преступления, совершаемые с использованием информационно-коммуникационных технологий. 2. Способы совершения киберпреступлений и особенности правоприменительной практики (ст. ст. 212, 209, 222, 340, главы 31 УК Республики Беларусь). 3. Подмена видео- и (или) аудиоинформации с применением элементов искусственного интеллекта как способ совершения преступлений. 4. Значение сетевой адресации (IP, MAC, DNS) в противодействии киберпреступности. 5. Особенности поиска оперативно-значимой информации из открытых источников сети Интернет, социальных сетей и DarkNet.		2		Устный опрос
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). 4. Составление запросов операторам электросвязи на получение информации.			2	Выполнение практических заданий
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.			2	Выполнение практических заданий
5	**Компьютерная информация: обнаружение и анализ**	**2**	**2**	**10**	
5.1	1. Средства компьютерной техники	2			

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	(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.				
5.2	1. Компьютерная информация: понятие, особенности, сетевые идентификаторы. 2. Особенности обнаружения и фиксации компьютерной информации на СКТ, находящихся во выключенном и включенном состоянии. 3. Особенности выгрузки данных сетевых аккаунтов (соцсети, мессенджеры, облачные сервисы). 4. Программно-техническое обеспечение осмотра и анализа СКТ.		2		Устный опрос
5.3	1. Анализ СКТ (электронных носителей информации) средствами операционной системы. 2. Анализ системных файлов, файлов реестра, хронологии событий операционной системы.			2	Выполнение практических заданий
5.4	1. Изучение функционального назначения прикладного программного обеспечения «НИРСОФТ». 2. Анализ СКТ с использованием прикладного программного обеспечения «НИРСОФТ».			2	Выполнение практических заданий
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»).			2	Выполнение практических заданий
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			2	Выполнение практических заданий

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Форма контроля знаний
		лекции	семинарские	практические	
	программно-технического комплекса «Мобильный криминалист»).				
5.7	1. Осмотр компьютерной информации (программно-технические аспекты): интернет-ресурс; электронная почта (E-mail).			2	Выполнение практических заданий
	Итого в 7 семестре	**10**	**10**	**28**	
	Форма промежуточной аттестации				**Экзамен**
	Общее количество по учебной дисциплине	**10**	**10**	**28**	**5**

Приложение 2

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

5. 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.

6. 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.

Дополнительная литература

7. 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.

8. Основы кибербезопасности: учебное пособие. / [А. А. Страхов и др.; рук. авт. кол. А. А. Страхов]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2023. – 208 с.

Нормативные правовые акты[2]

9. 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, 2024.

10. 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, 2024.

11. О кибербезопасности: утв. Указом Президента Республики Беларусь 14 февр. 2023 г., № 40 // Консультант Плюс : Беларусь. [Электронный ресурс] / ООО «ЮрСпектр», Национальный Центр правовой информации Республики Беларусь. – Минск, 2024.

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, 2024.

13. 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. –

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

Минск, 2024.

14. 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.

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

УТВЕРЖДАЮ
врио Начальник учреждения
образования «Академия
Министерства внутренних дел
Республики Беларусь»
генерал-майор милиции
А.В.Астрейко
08.07.2025 А.В.Бакиан

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
по учебной дисциплине «Противодействие киберпреступности и основы защиты информации» модуль «Информационная безопасность» по специальностям 6-05-0421-01 (1-24 01 02) Правоведение, 6-05-0421-03 (1-24 01 03) Экономическое право

№№ п/п	Дополнения и изменения	Основание
1.	Изложить подраздел «Содержание учебного материала» раздела «Пояснительная записка» в новой редакции (приложение 1).	П. 12 Плана реализации предложений, поступивших в рамках УМС профессорско-преподавательского состава Академии МВД с участием представителей заказчиков кадров Решение кафедры (протокол № 9 от 03.04.2025)
2.	Изложить учебно-методическую карту учебной дисциплины для дневной формы получения высшего образования для специальностей 6-05-0421-01 (1-24 01 02) Правоведение 6-05-0421-03 (1-24 01 03) Экономическое право в новой редакции (приложение 2).	
3.	Изложить учебно-методическую карту учебной дисциплины для заочной формы получения высшего образования по специальности 6-05-0421-01 (1-24 01 02) «Правоведение» профилизации «Судебно-прокурорско-следственная деятельность», «Административно-правовая деятельность» (срок получения высшего образования 5 лет) для набора 2022 года в новой редакции (приложение 3).	
4.	Изложить учебно-методическую карту учебной дисциплины для заочной формы получения высшего образования по специальности 6-05-0421-01 (1-24 01 02) «Правоведение» (срок получения высшего образования 3 года, для наборов 2022 и 2023 годов) в новой редакции (приложение 4).	
5.	Изложить раздел «Информационно-методическая часть» в новой редакции (приложение 5).	

Учебная программа пересмотрена и одобрена на заседании кафедры информационного права факультета криминальной милиции учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 9 от 3 апреля 2025 года).

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

Одобрены и рекомендованы к утверждению научно-методическим советом учреждения образования «Академия Министерства внутренних дел Республики Беларусь» (протокол № 13 от 18.06.2025 года).

Приложение 1

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

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

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.

Тема 2. Каналы утечки информации и безопасность информационных систем

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.

Тема 3. Аппаратное и программное обеспечение защищенных компьютерных систем

Операционные системы и их защищенность. Установка операционных систем на персональный компьютер. Особенности фундаментального подхода к построению архитектуры системы защиты.

Методы и средства защиты информации в компьютерных системах.

Тема 4. Основы противодействия киберпреступности

Современные подходы к определению понятия и содержанию киберпреступности. Способы совершения киберпреступлений (в т. ч. сопряженных с подменой видео- и (или) аудиоинформации с применением элементов искусственного интеллекта). Особенности предупреждения киберпреступлений. Глобальная компьютерная сеть Интернет: структура, основные понятия и термины, необходимые в работе сотрудника правоохранительных органов. Структура построения модели OSI. Технологии NAT, PAT и VPN. Основы поисковой деятельности в сети Интернет: использование поисковых ресурсов; использование иных информационных систем.

Тема 5. Компьютерная информация: обнаружение и анализ

Понятие компьютерной информации и ее классификация.

Цифровые идентификаторы и их характеристика. Обнаружение и анализ компьютерной информации. Современные программно-аппаратные средства исследования и анализа 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.

Приложение 2

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Противодействие киберпреступности и основы защиты информации»

модуля «Информационная безопасность»
для специальностей 6-05-0421-01 (1-24 01 02) Правоведение
6-05-0421-03 (1-24 01 03) Экономическое право
дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия		
7 семестр						
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**	**2**			
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2				
1.2	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.		2			Устный опрос
Тема 2	**Каналы утечки информации и безопасность информационных систем**	**2**	**2**			
2.1	1. Основные угрозы безопасности информационных систем. 2. Каналы утечки информации: виды, содержание, особенности реализации. 3. Способы и средства предотвращения утечки информации.	2				
2.2	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. Основные подходы к защите информации в Едином цифровом пространстве МВД Республики Беларусь.		2			Устный опрос
Тема 3	**Аппаратное и программное обеспечение защищенных компьютерных систем**	**2**	**2**	**12**		

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия		
3.1	1. Операционные системы и их защищенность. 2. Методы и средства защиты информации в компьютерных системах.	2				
3.2	1. Политика информационной безопасности единой цифровой платформы МВД Республики Беларусь. 2. Особенности фундаментального подхода к построению архитектуры системы защиты. Подсистемы безопасности операционной системы. 3. Технологии NAT, PAT и VPN. 4. Защита периметра компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы). Обнаружение атак (опасных действий нарушителей) и оперативное реагирование. 5. Установка операционных систем на ПК.		2			Устный опрос
3.3	1. Антивирусное программное обеспечение. 2. Резервное копирование. Создание образа системы.			2		Опрос, выполнение практических заданий
3.4	1. Шифрование данных средствами прикладных программных продуктов. 2. Создание и использование защищенных криптоконтейнеров.			2		Опрос, выполнение практических заданий
3.5	1. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force. 2. Стеганографические методы защиты информации.			2		Опрос, выполнение практических заданий
3.6	1. Средства виртуализации: установка, настройка и использование. 2. Гостевая ОС Linux: установка и администрирование. Онлайн-определение параметров User Agent.			2		Опрос, выполнение практических заданий
3.7	1. ОС Linux: установка и настройка. 2. Изучение функциональных особенностей ОС Linux: общий аудит безопасности; анализ уязвимостей; сетевой мониторинг.			2		Опрос, выполнение практических заданий
3.8	1. Организация безопасного хранения паролей в защищаемых компьютерных системах. 2. Методы восстановления удаленной информации с электронных носителей с использованием специального программного обеспечения. Порядок удаления информации программными способами без возможности ее восстановления. 3. Проверка и удаление следов активности пользователя в системе.			2		Опрос, выполнение практических заданий
Тема 4	**Основы противодействия киберпреступности**	**2**	**2**	**4**		
4.1	1. Киберпреступность: сущность и содержание,	2				

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия		
	особенности противодействия. 2. Способы совершения киберпреступлений (в т. ч. сопряженных с подменой видео- и (или) аудиоинформации с применением элементов искусственного интеллекта). 3. Глобальная сеть Интернет как среда совершения киберпреступлений. 4. Особенности получения информации из открытых источников сети Интернет для решения служебных задач.					
4.2	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. 5. Использование специальной терминологии (сленг) в сфере противодействия киберпреступности.		2			Устный опрос
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 анонимайзеров. 4. Составление запросов на получение информации.			2		Опрос, выполнение практических заданий заданий
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.			2		Опрос, выполнение практических заданий заданий
5	**Компьютерная информация: обнаружение и анализ**	**2**	**2**	**12**		
5.1	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.	2				
5.2	1. Понятие компьютерной информации. 2. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на компьютере, находящемся во включенном состоянии.		2			Устный опрос

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия		
	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.					
5.3	1. Анализ СКТ (электронных носителей информации) средствами операционной системы. 2. Анализ системных файлов, файлов реестра, хронологии событий операционной системы.			2		Опрос, выполнение практических заданий заданий
5.4	1. Анализ СКТ с использованием прикладного программного обеспечения («НИРСОФТ»). 2. Анализ сетевой активности с использованием прикладного программного обеспечения «Wireshark».			2		Опрос, выполнение практических заданий заданий
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»).			2		Опрос, выполнение практических заданий заданий
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»).			2		Опрос, выполнение практических заданий заданий
5.7	1. Осмотр компьютерной информации (программно-технические аспекты): интернет-ресурс; электронная почта (E-mail).			2		Опрос, выполнение практических заданий заданий
5.8	1. Решение комплексной задачи.			2		Опрос, выполнение практических заданий заданий
	Итого в 7 семестре	**10**	**10**	**28**		
	Общее количество аудиторных часов по учебной дисциплине:	**10**	**10**	**28**		
	Форма текущей аттестации по учебной дисциплине в 7 семестре:	устный опрос по темам №№ 1-5				
	Форма промежуточной аттестации в 7 семестре:	Экзамен (устно)				

Приложение 3

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Противодействие киберпреступности и основы защиты информации»

модуля «Информационная безопасность»
для специальности 6-05-0421-01 (1-24 01 02) «Правоведение»
(профилизации «Судебно-прокурорско-следственная деятельность»,
«Административно-правовая деятельность»)
заочная форма получения высшего образования
(срок получения образования 5 лет)
(для набора 2022 года)

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Самостоятельная работы	Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия			
9 семестр							
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**					
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2					
	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.				с/р	1, стр. 2-8; 7; 8; 11	
Тема 2	**Каналы утечки информации и безопасность информационных систем**						
	1. Основные угрозы безопасности информационных систем. 2. Каналы утечки информации: виды, содержание, особенности реализации. 3. Способы и средства предотвращения утечки информации. 4. Угрозы информационной безопасности и их источники. Неформальная модель возможного нарушителя информационной безопасности. 5. Каналы утечки информации: виды, содержание, особенности реализации.				с/р	1, стр. 35-43; 2, стр. 101-166	

	6. Способы обнаружения (выявления) технических каналов утечки информации. 7. Основные подходы к защите информации в Едином цифровом пространстве МВД Республики Беларусь						
Тема 3	**Аппаратное и программное обеспечение защищенных компьютерных систем**			**4**			
3.1	1. Антивирусное программное обеспечение. 2. Резервное копирование. Создание образа системы.			2			Опрос, выполнение практических заданий
3.2	1. Шифрование данных средствами прикладных программных продуктов. 2. Создание и использование защищенных криптоконтейнеров.			2			Опрос, выполнение практических заданий
	1. Операционные системы и их защищенность. 2. Методы и средства защиты информации в компьютерных системах. 3. Политика информационной безопасности единой цифровой платформы МВД Республики Беларусь. 4. Особенности фундаментального подхода к построению архитектуры системы защиты. Подсистемы безопасности операционной системы. 5. Технологии NAT, PAT и VPN. 6. Защита периметра компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы). Обнаружение атак (опасных действий нарушителей) и оперативное реагирование. 7. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force. 8. Стеганографические методы защиты информации. 9. Средства виртуализации: установка, настройка и использование. 10. Гостевая ОС Linux: установка и администрирование. Онлайн-определение параметров User Agent. 11. ОС Linux: установка и настройка. 12. Изучение функциональных особенностей ОС Linux: общий аудит безопасности; анализ уязвимостей; сетевой мониторинг. 13. Организация безопасного хранения паролей в защищаемых компьютерных системах.				с/р	1, стр. 82-109; 2, стр. 124-133; 4, стр. 55-59	
	14. Методы восстановления удаленной информации с электронных носителей с использованием специального программного обеспечения. Порядок удаления информации программными способами без возможности ее восстановления. 15. Проверка и удаление следов активности пользователя в системе.						
Тема 4	**Основы противодействия киберпреступности**			**4**			

4.1	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 анонимайзеров. 4. Составление запросов на получение информации.			2			Опрос, выполнение практических заданий
	ИТОГО в 9 семестре	**2**		**6**			
	10 семестр						
4.2	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.			2			
	1. Киберпреступность: сущность и содержание, особенности противодействия. 2. Способы совершения киберпреступлений (в т. ч. сопряженных с подменой видео- и (или) аудиоинформации с применением элементов искусственного интеллекта). 3. Глобальная сеть Интернет как среда совершения киберпреступлений. 4. Особенности получения информации из открытых источников сети Интернет для решения служебных задач. 5. Классификация преступлений, совершаемых с использованием информационно-коммуникационных технологий. 6. Способы совершения киберпреступлений и особенности правоприменительной практики. 7. Значение сетевой адресации (IP, MAC, DNS) в противодействии киберпреступности. 8. Особенности поиска оперативно-значимой информации из открытых источников сети Интернет, социальных сетей и DarkNet. 9. Использование специальной терминологии (сленг) в сфере противодействия киберпреступности.				с/р	1, стр. 145-200; 2; 3; 4	
5	**Компьютерная информация: обнаружение и анализ**			**2**			
5.1	1. Изучение структуры и содержания информации, извлеченной из исследуемых СКТ. 2. Анализ информации, извлеченной из исследуемых СКТ (на примере программно-технического комплекса «Мобильный криминалист»).			2			Опрос, выполнение практических заданий

	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. 4. Понятие компьютерной информации. 5. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на компьютере, находящемся во включенном состоянии. 6. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на компьютере, находящемся в выключенном состоянии. 7. Особенности исследования и использования компьютерной информации, содержащей электронно-цифровые следы. 8. Программно-техническое обеспечение осмотра и анализа СКТ. 9. Анализ СКТ (электронных носителей информации) средствами операционной системы. 10. Анализ системных файлов, файлов реестра, хронологии событий операционной системы. 11. Анализ СКТ с использованием прикладного программного обеспечения («НИРСОФТ»). 12. Анализ сетевой активности с использованием прикладного программного обеспечения «Wireshark». 13. Изучение структуры и содержания логических и физических образов, извлеченных из исследуемых мобильных устройств. 14. Анализ информации, извлеченной из мобильных устройств (на примере программно-технического комплекса «Мобильный криминалист»). 15. Решение комплексной задачи.				с/р	1, стр. 201-224; 4, стр. 55-60; 5, стр. 68-120	
	ИТОГО в 10 семестре			**4**			
	Общее количество аудиторных часов по учебной дисциплине:	**2**		**10**			
	Форма текущей аттестации по учебной дисциплине в 10 семестре:	устный опрос по темам №№ 1-5					
	Форма промежуточной аттестации по учебной дисциплине в 10 семестре:	Экзамен (устно)					

Приложение 4

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ
«Противодействие киберпреступности и основы защиты информации»

модуля «Информационная безопасность»
для специальности 6-05-0421-01 (1-24 01 02) Правоведение
заочная форма получения высшего образования
срок получения высшего образования 3 года
(для наборов 2022 и 2023 годов)

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Самостоятельная работы	Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия			
9 семестр							
Тема 1	**Правовые и организационно-технические меры обеспечения информационной безопасности в системе национальной безопасности Республики Беларусь**	**2**					
1.1	1. Понятие, содержание информационной безопасности. 2. Правовое обеспечение информационной безопасности. 3. Основные направления обеспечения информационной безопасности.	2					
	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.				с/р	1, стр. 2-8; 7; 8; 11	
Тема 2	**Каналы утечки информации и безопасность информационных систем**						
	1. Основные угрозы безопасности информационных систем. 2. Каналы утечки информации: виды, содержание, особенности реализации. 3. Способы и средства предотвращения утечки информации. 4. Угрозы информационной безопасности и их источники. Неформальная модель возможного нарушителя информационной безопасности. 5. Каналы утечки информации: виды, содержание, особенности реализации.				с/р	1, стр. 35-43; 2, стр. 101-166	
	6. Способы обнаружения (выявления) технических каналов утечки информации. 7. Основные подходы к защите информации в Едином цифровом пространстве МВД Республики Беларусь.						

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Самостоятельная работы	Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия			
Тема 3	**Аппаратное и программное обеспечение защищенных компьютерных систем**						
	1. Операционные системы и их защищенность. 2. Методы и средства защиты информации в компьютерных системах. 3. Политика информационной безопасности единой цифровой платформы МВД Республики Беларусь. 4. Особенности фундаментального подхода к построению архитектуры системы защиты. Подсистемы безопасности операционной системы. 5. Технологии NAT, PAT и VPN. 6. Защита периметра компьютерных сетей (фильтрация трафика, скрытие внутренней структуры и адресации, противодействие атакам на внутренние ресурсы). Обнаружение атак (опасных действий нарушителей) и оперативное реагирование. 7. Антивирусное программное обеспечение. 8. Резервное копирование. Создание образа системы. 9. Шифрование данных средствами прикладных программных продуктов. 10. Создание и использование защищенных криптоконтейнеров. 11. Создание зашифрованных архивов данных. Восстановление пароля методами подбора по словарю и Brute-force. 12. Стеганографические методы защиты информации. 13. Средства виртуализации: установка, настройка и использование. 14. Гостевая ОС Linux: установка и администрирование. Онлайн-определение параметров User Agent. 15. ОС Linux: установка и настройка. 16. Изучение функциональных особенностей ОС Linux: общий аудит безопасности; анализ уязвимостей; сетевой мониторинг. 17. Организация безопасного хранения паролей в защищаемых компьютерных системах.				с/р	1, стр. 82-109; 2, стр. 124-133; 4, стр. 55-59	
	18. Методы восстановления удаленной информации с электронных носителей с использованием специального программного обеспечения. Порядок удаления информации программными способами без возможности ее восстановления. 19. Проверка и удаление следов активности пользователя в системе.						
	ИТОГО в 5 семестре	**2**					

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Самостоятельная работы	Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия			
10 семестр							
Тема 4	**Основы противодействия киберпреступности**	**2**		**4**			
4.1	1. Киберпреступность: сущность и содержание, особенности противодействия. 2. Способы совершения киберпреступлений (в т. ч. сопряженных с подменой видео- и (или) аудиоинформации с применением элементов искусственного интеллекта). 3. Глобальная сеть Интернет как среда совершения киберпреступлений. 4. Особенности получения информации из открытых источников сети Интернет для решения служебных задач.	2					Опрос, выполнение практических заданий
4.2	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 анонимайзеров. 4. Составление запросов на получение информации.			2			Опрос, выполнение практических заданий
4.3	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.			2			Опрос, выполнение практических заданий
	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. 5. Использование специальной терминологии (сленг) в сфере противодействия киберпреступности.				с/р	1, стр. 145-200; 2; 3; 4	
5	**Компьютерная информация: обнаружение и анализ**			**4**			
5.1	1. Изучение структуры и содержания информации, извлеченной из исследуемых СКТ. 2. Анализ информации, извлеченной из исследуемых СКТ (на примере программно-технического комплекса «Мобильный криминалист»).			2			Опрос, выполнение практических заданий
5.2	1. Осмотр компьютерной информации (программно-технические аспекты):			2			

Номер раздела, темы	Название раздела, темы, наименование учебных вопросов	Количество аудиторных часов			Самостоятельная работы	Источник, страницы	Форма контроля знаний
		Лекции	Семинарские занятия	Практические занятия			
	интернет-ресурс; электронная почта (E-mail).						
	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. 4. Понятие компьютерной информации. 5. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на компьютере, находящемся во включенном состоянии. 6. Особенности обнаружения и фиксации компьютерной информации, содержащей электронно-цифровые следы на компьютере, находящемся в выключенном состоянии. 7. Особенности исследования и использования компьютерной информации, содержащей электронно-цифровые следы. 8. Программно-техническое обеспечение осмотра и анализа СКТ. 9. Анализ СКТ (электронных носителей информации) средствами операционной системы. 10. Анализ системных файлов, файлов реестра, хронологии событий операционной системы. 11. Анализ СКТ с использованием прикладного программного обеспечения («НИРСОФТ»). 12. Анализ сетевой активности с использованием прикладного программного обеспечения «Wireshark». 13. Изучение структуры и содержания логических и физических образов, извлеченных из исследуемых мобильных устройств. 14. Анализ информации, извлеченной из мобильных устройств (на примере программно-технического комплекса «Мобильный криминалист»). 15. Осмотр компьютерной информации (программно-технические аспекты): интернет-ресурс; электронная почта (E-mail). 16. Решение комплексной задачи.				с/р	1, стр. 201-224; 4, стр. 55-60; 5, стр. 68-120; 12	
	ИТОГО в 6 семестре	**2**		**8**			
	Общее количество аудиторных часов по учебной дисциплине:	**4**		**8**			
	Форма текущей аттестации по учебной дисциплине в 6 семестре:	устный опрос по темам №№ 1-5					
	Форма промежуточной аттестации по учебной дисциплине в 6 семестре:	Экзамен (устно)					

Приложение 5

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Основная литература

1. Противодействие киберпреступности и основы защиты информации : учебное пособие / Д.Н. Лахтиков, Боровик П.Л., Пикта В.И., (общ. ред. Д.Н. Лахтиков); учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь» – Минск : Академия МВД, 2024. – 259 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. Противодействие киберпреступности и основы защиты информации: электронный учебно-методический комплекс // Локальная сеть Академии: atk «Электронная Академия».

5. Организация расследования преступлений в сфере высоких технологий : учебное пособие / П. В. Гридюшко [и др.]; под общ.ред. И. Г. Мухина ; учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Академия МВД, 2016. – 154 с.

6. Основы кибербезопасности: учебное пособие. / [А. А. Страхов и др.; рук. авт. кол. А. А. Страхов]. – М. : Московский университет МВД России имени В.Я. Кикотя, 2023. – 208с.

Нормативные правовые акты[3]

1. О ведомственных сетях передачи данных, глобальной компьютерной сети Интернет, файлообменном сервисе и ведомственной электронной почте : Приказ МВД Республики Беларусь, 17 октября 2024 г., № 349.

2. Об утверждении Концепции национальной безопасности Республики Беларусь: Решение всебелорусского народного собрания, 25 апреля 2024 г., № 5.

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

4. О кибербезопасности: утв. Указом Президента Республики Беларусь 14 февр. 2023 г., № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.

5. О концепции информационной безопасности Республики Беларусь : постановление Совета безопасности Республики Беларусь, 18 марта 2019 г., №1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац.

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

центр правовой информ. Респ. Беларусь. – Минск, 2025.

6. О мерах по совершенствованию использования национального сегмента сети Интернет: утв. Указом Президента Республики Беларусь 1 февр. 2010 г., № 60 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.

7. Об информации, информатизации и защите информации : Закон Республики Беларусь, 10 ноября 2008 г., №455-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2025.