МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ О.Е. КУТАФИНА (МГЮА)»

Кафедра уголовного права

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

КИБЕРНЕТИЧЕСКАЯ ПРЕСТУПНОСТЬ

Б1.В.ДВ.04.02

год набора 2025

Код и наименование направления подготовки:	40.04.01 Юриспруденция
Уровень высшего образования:	магистратура
Направленность (профиль) ОПОП ВО:	Уголовное право и уголовное судопроизводство
Форма (формы) обучения:	очная, заочная
Квалификация:	магистр

Москва – 2025

Программа одобрена на заседании кафедры
от «29» января 2025 г., протокол № 5

Автор:

Мацкевич И.М. - д.ю.н., профессор, заведующий кафедрой криминологии и уголовно-исполнительного права

Рецензент:

Грачёва Ю.В. – д.ю.н., профессор

Мацкевич И.М.
Кибернетическая преступность: рабочая программа / И.М. Мацкевич. – М. Издательский центр Университета имени О. Е. Кутафина (МГЮА), 2025. - 28 с.

Программа составлена в соответствии с требованиями ФГОС ВО по направлению подготовки 40.04.01 Юриспруденция
Программа адаптирована кафедрой уголовного права и криминологии для Оренбургского института (филиала) Университета имени О.Е. Кутафина (МГЮА).

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Цели и задачи освоения дисциплины (модуля)

Целями освоения дисциплины «Кибернетическая преступность» являются:

1) получения системного знания о предупреждении и профилактики финансовой преступности;

2) формирования навыков по обеспечению личной безопасности граждан и предпринимателей в области финансовой деятельности;

3) правильная организация безопасного предпринимательства и личного поведения, связанного с финансовыми тратами, включая взаимодействие в соответствии с действующим законодательством с банками и другими государственными и общественными институтами;

4) формирование навыков по обеспечению системы безопасного поведения людей в области финансов, защиты от финансового мошенничества и других экономических преступлений;

5) воспитание нетерпимого отношения к совершению правонарушений (преступлений), посягающих на безопасность в области финансовой деятельности.

Задачи дисциплины «Кибернетическая преступность» состоят в следующем:

- качественной подготовке конкурентоспособных и компетентных профессиональных юристов, обладающих высоким уровнем правовой культуры и правосознания, знаниями в области правоохранительной и правоприменительной деятельности;

- приобретении умения применения полученных знаний в правоприменительной, правоохранительной, экспертно-консультационной, организационно-управленческой и научно-исследовательской деятельности.

Основными видами деятельности, к которым осуществляется подготовка в рамках дисциплины, являются:

а) правоприменительная:

- обоснование и принятие в пределах должностных обязанностей решений, а также совершение действий, связанных с реализацией правовых норм;

- составление юридических документов;

б) правоохранительная:

- обеспечение законности, правопорядка, безопасности личности, общества и государства;

- защита частной, государственной, муниципальной и иныхформ собственности;

- предупреждение, пресечение, выявление финансовых преступлений;

- защита прав и законных интересов юридических лиц и от-

дельных граждан;

в) экспертно-консультационная деятельность:

- оказание юридической помощи, консультирование по вопросам права;

г) организационно-управленческая деятельность:

- осуществление организационно-управленческих функций;

д) научно-исследовательская:

- участие в проведении научных исследований в соответствии с профилем своей профессиональной деятельности.

1.2. Место дисциплины (модуля) в структуре ОПОП ВО

Дисциплина (модуль) «Кибернетическая преступность» (Б1.В.ДВ.04.02) относится к Блоку 1, к части, формируемой участниками образовательных отношений основной профессиональной образовательной программы высшего образования, элективные дисциплины.

Приступая к изучению дисциплины, обучающийся должен обладать теоретическими знаниями в области теории права, гражданского права, уголовного права, финансового права, административного права, трудового права, гражданского процессуального права, арбитражно-процессуального права, уголовного процессуального права, криминалистики, криминологии и психологии.

При изучении учебной дисциплины обучающийся, в частности, должен обладать следующими входными знаниями и умениями:

в области знаний: объяснить понятие кибернетической преступности и составляющие его признаки, рассмотреть особенности теневой экономики; обозначить критерии классификаций причин и условий; дать основы профилактики правонарушений и преступлений, связанных с использованием компьютеров и цифровой деятельностью; изучить виды компьютерных преступлений; определить мошенничества с использованием компьютеров и другие преступления, связанные с цифровой деятельностью;

в области понимания: раскрыть суть цифровой экономики и деятельности, связанной с использованием компьютеров; раскрыть сутьтеневой экономики; объяснить специфику определения причин и условий компьютерных преступлений; дифференцировать возможности использования юридических знаний для предупреждения компьютерных преступлений;

в области умения, навыка: осуществлять информационно-поисковую, аналитическую деятельность по обеспечения безопасности предпринимательской деятельности и деятельности, связанной с использованием компьютеров; самостоятельно принимать решения о виктимологической профилактике; толковать и правильно применять правовые нормы в области цифровых технологий; предупреждать компьютерные преступления, выявлять и устранять причины и условия, способствующие их совершению; владеть навыками: поиска, анализа и обобщения получаемой

информации, самостоятельной научной работы, разрешения казусов и конфликтных ситуаций.

Дисциплина «Кибернетическая преступность» является необходимым элементом подготовки будущего магистра, способствует более глубокому усвоению остальных дисциплин магистерской программы, а также организации процесса написания магистерской диссертации.

1.3. Формируемые компетенции и индикаторы их достижения (планируемые результаты освоения дисциплины (модуля))

По итогам изучения дисциплины (модуля) « Экономическая преступность» обучающийся должен обладать следующими компетенциями в соответствии с ФГОС ВО:

Универсальные компетенции:

- Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий (УК-1);
- Способен управлять проектом на всех этапах его жизненного цикла (УК-2).

Профессиональные компетенции:

- Способен разрабатывать нормативные правовые и локальные правовые акты в конкретных сферах юридической деятельности (ПК-1);
- Способен планировать и организовывать научные исследования, участвовать в научно-исследовательских работах по проблемам права; способен разрабатывать собственный научный проект (ПК-5).

Разделы (темы) дисциплины (модуля)	**Код и наименование формируемых компетенций**	**Индикатор достижения компетенций (планируемый результат освоения дисциплины (модуля))**
Общая характеристика кибернетической преступности Понятие и виды кибернетической преступности Личность кибернетическойго преступника Причины кибернетической преступности	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий УК-2 Способен управлять проектом на всех этапах его жизненного цикла	ИУК 1.1Анализирует проблемную ситуацию как систему, выявляя ее составляющие и связи между ними ИУК 1.3. Критически оценивает надежность источников информации, работает с противоречивой информацией из разны источников ИУК 1.4.Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов ИУК 2.1. Формулирует на основе поставленной проблемы проектную задачу и способ ее решения через реализацию проектного управления ИУК 2.2.Разрабатывает концепцию проекта в рамках обозначенной проблемы: формулирует цель, задачи,

Кибернетическая преступность в зарубежных странах Предупреждение кибернетической преступности	ПК-1 Способен разрабатывать нормативные правовые и локальные правовые акты в конкретных сферах юридической деятельности (ПК-5) Способен планировать и организовывать научные исследования, участвовать в научно-исследовательских работах по проблемам права; способен разрабатывать собственный научный проект	обосновывает актуальность, значимость, ожидаемые результаты и возможные сферы их применения ИПК ИПК 1.2.Применяет основные приемы законодательной техники при подготовке нормативных правовых актов в сфере своей профессиональной деятельности ИПК 5.1.Показывает способность проводить анализ и обобщение результатов научно-исследовательских работ с использованием современных достижений научного знания, передового отечественного и зарубежного опыта

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1. Тематические планы

Общая трудоемкость дисциплины составляет 3 зачетные единицы, 108 часов.

2.1.1. ТЕМАТИЧЕСКИЙ ПЛАН (для очной формы обучения)

№ п/п	Раздел (тема) учебной дисциплины	Семестр	Виды учебной деятельности и трудоемкость (в часах)			Образовательные технологии	Формы текущего контроля
			Лекции	Практ. занятия/ Лаборат.	СРС		
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	3	2		13	лекция-дискуссия, лекция-презентация, информационная, обобщающая, проблемная лекция	самостоятельная работа, эссе, реферат, коллоквиум
2	Понятие и виды кибернетической преступности	3		2(2)	13	работа в малых группах, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
3	Личность киберпреступника	3		2	13	разбор конкретных ситуаций, практика публичного выступления,	самостоятельная работа, эссе, реферат, колло-

						«мозговой штурм», использование видео- и компьютерных пособий	квиум

4	Причины кибернетической преступности	3		2	13	работа в малых группах, «займи позицию», разбор конкретных ситуаций, использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
5	Криминологическая характеристика хакерских атак	3		2	13	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
6	Кибернетическая преступность в зарубежных странах			2	13	работа в малых группах, «займи позицию», разбор конкретных ситуаций, использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
7	Предупреждение кибернетической преступности			2	14	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
	ВСЕГО		**2**	**12(2)**	**92**		зачет

Дисциплина «Кибернетическая преступность» изучается в течение одного семестра. Итоговая аттестация осуществляется в форме зачета.

2.1.2. Тематический план для заочной формы обучения

№ п/п	Раздел (тема) учебной дисциплины	Семестр	Виды учебной деятельности и трудоемкость (в часах)			Образовательные технологии	Формы текущего контроля
			Лекции	Практ. занятия/ Лаборат.	СРС		
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	3	2		13	лекция-дискуссия, лекция-презентация, информационная, обобщающая, проблемная лекция	самостоятельная работа, эссе, реферат, коллоквиум
2	Понятие и виды кибернетической преступности	3			13	работа в малых группах, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
3	Личность киберпреступника	3		-	13	разбор конкретных ситуаций, практика публичного выступления, «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
4	Причины кибернетической преступности	3		2	13	**Лаборат. занятие.** работа в малых группах, использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум

5	Криминологическая характеристика хакерских атак	3		2	13	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
6	Кибернетическая преступность в зарубежных странах			2	13	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
7	Предупреждение кибернетической преступности			2	14	разбор конкретных ситуаций, «займи позицию», «мозговой штурм», использование видео- и компьютерных пособий	самостоятельная работа, эссе, реферат, коллоквиум
	Зачет 4 ч.						
	ВСЕГО		**2**	**8(2)**	**92**		

Учебная дисциплина «Кибернетическая преступность» изучается в течение одного семестра. Итоговая аттестация осуществляется в форме зачета.

Содержание дисциплины (программа курса)

(для всех форм обучения)

№ п/п	Наименование раздела дисциплины	Содержание раздела
1	Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	Особенности кибернетической преступности. Взаимосвязь с экономической преступностью. Уголовно-правовая характеристика компьютерных преступлений. Структура и характер кибернетической преступности. Виды латентной кибернетической преступности. Сущность и содержание криминологической безопасности цифровой деятельности. Криминологическая безопасность поведения граждан, связанных с использованием компьютеров и цифровых технологий. Значение криминологии в ее обеспечении. Взаимосвязь криминологии в обеспечении компьютерной безопасности с науками уголовно-правового цикла, с науками гражданско-правового цикла, с науками государственно-правового цикла: задачи и особенности.
2	Понятие и виды кибернетической преступности	История кибернетической преступности. Теневая экономика и теневая деятельность, связанная с использованием цифровых технологий. Понятие, признаки и виды кибернетической преступности. Тенденции кибернетической преступности. Предупреждение корпоративных конфликтов и роль в них компьютеров и цифровой технологии. Электронные деньги и другие современные компьютерные средства: их роль в совершении преступлений.
3	Личность кибер-преступника	Понятие и структура личности кибер-преступника. Классификация и типология различных групп и типов кибер-преступников. Механизм преступного поведения личности кибер-преступника. Виды виктимологического поведения предпринимателей и значение его изучения. Компьютерная виктимность гражданина: понятие и характерные черты. Предупреждение виктимологического поведения руководителя предприятия и работников предприятия. Правовое обеспечение защиты предпринимателей и обычных граждан от компьютерных преступлений: криминологическая характеристика.
4	Причины кибернетической преступности	Детерминация кибернетической преступности. Классификация причин и условий кибернетической преступности. Социальная обусловленность кибернетической преступности. Влияние личностных факторов на кибернетическую преступность. Криминологическая характери-

		стика основных нормативных правовых актов, регламентирующих использование компьютеров и другую цифровую деятельность. Особенности работы современных коммуникационных систем: криминологическая характеристика.
5	Криминологическая характеристика хакерских атак	Криминологическая характеристика хакерской деятельности и других видов компьютерных преступлений. Взаимосвязь компьютерных преступлений с должностной преступностью и коррупцией. Криминологическая характеристика коррупции. Взаимосвязь хакерской деятельности с организованной преступностью. Криминологическая характеристика компьютерной организованной преступности. Взаимосвязь компьютерных мошенничеств с незаконной предпринимательской деятельностью. Криминологическая характеристика незаконной предпринимательской деятельности.
6	Кибернетическая преступность в зарубежных странах	Общая характеристика кибернетической преступности развитых стран. Общая характеристика кибернетической преступности стран с переходной экономикой. Общая характеристика кибернетической преступности в других странах. Структура кибернетической преступности за рубежом. Борьба с кибернетической преступностью за рубежом. Соотношение кибернетической и организованной преступности за рубежом. Электронные деньги и компьютерные мошенничества в России и за рубежом: сравнительный анализ.
7	Предупреждение кибернетической преступности	Теория предупреждения кибернетической преступности: понятие, признаки и виды. Специальные субъекты предупреждения кибернетической преступности. Методика проведения статистических исследований деятельности, связанной с цифровой экономикой. Методы проведения социологических опросов среди пользователей компьютерными сетями. Криминология интернета. Проведение анонимных опросов и анализ их результатов. Интервью, как средство предупреждения деликтов, правонарушений и преступлений. Граждане, склонные к неоправданному рискованному финансовому поведению: криминологический анализ.

2.2. Занятия лекционного типа (для очной и заочной форм обучения)

Наименование лекции	Объем часов	Тематика лекции	Задания для подготовки к лекции
Общая характеристика кибернетической преступности и взаимосвязь с экономической преступностью	2	Сущность и содержание криминологической безопасности цифровой деятельности. Криминологическая безопасность поведения граждан, связанных с использованием компьютеров и цифровых технолгий. Значение криминологии в ее обеспечении. Взаимосвязь криминологии в обеспечении компьютерной безопасности с науками уголовно-правового цикла, с науками гражданско-правового цикла, с науками государственно-правового цикла: задачи и особенности. Значение криминологических основ безопасности компьютерной деятельности в работе современного предпринимателя и обычного гражданина. .	изучить и проанализировать: - нормативные акты в части правовой регламентации банковской деятельности; - следственную и судебную практику, связанную с предупреждением деликтов, правонарушений и преступлений в банковской и финансовой деятельности; - следственную и судебную практику, связанную с предупреждением деликтов, правонарушений и преступлений в банковской и финансовой деятельности.

2.3. Занятия семинарского типа для очной (14 часов) и заочной (10 часов) форм обучения

Наименование темы	Содержание практического занятия
Понятие и виды кибернетической преступности	История кибернетической преступности. Теневая экономика и теневая деятельность, связанная с использованием цифровых технологий. Понятие, признаки и виды кибернетической преступности. Тенденции кибернетической преступности. Предупреждение корпоративных конфликтов и роль в них компьютеров и цифровой технологии. Электронные деньги и другие современные компьютерные средства: их роль в совершении преступлений. *Задание для подготовки:* повторить основные положения криминологической теории, найти и изучить основные действующие криминологические нормативные правовые акты, направленные против кибернетической преступности и дать их классификацию, разобраться с тем, что понимается под теневой экономикой и как легализуются незаконно полученные деньги, посредством компьютерных технологий; изучить методы и способы отмывания денег и совершения компьютерных мошенничеств
Личность кибер-преступника	Понятие и структура личности кибер-преступника. Классификация и типология различных групп и типов кибер- преступников. Механизм преступного поведения личности кибер-преступника. Виды виктимологического поведения предпринимателей и значение его изучения
	Компьютерная виктимность гражданина: понятие и характерные черты. Предупреждение виктимологического поведения руководителя предприятия и работников предприятия. Правовое обеспечение защиты предпринимателей и обычных граждан от компьютерных преступлений: криминологическая характеристика. *Задание для подготовки:* повторить криминологическую теорию личности преступника, дать криминологическую характеристику личности кибер-преступника и построить его криминологических портрет, изучить нормативные правовые акты, касающиеся защиты свидетелей и потерпевших от кибернетических преступлений.

Причины кибернетической преступности	Детерминация кибернетической преступности. Классификация причин и условий кибернетической преступности. Социальная обусловленность кибернетической преступности. Влияние личностных факторов на кибернетическую преступность. Криминологическая характеристика основных нормативных правовых актов, регламентирующих использование компьютеров и другую цифровую деятельность. Особенности работы современных коммуникационных систем: криминологическая характеристика. *Задание для подготовки:* повторить теорию причинности в криминологии, изучить основные положения нормативных правовых актов, регламентирующих безопасную цифровую деятельность, а также специфику работы правоохранительных органов в этой области, определить нормативные правовые документы, направленные на выявление причин и условий противоправного поведения, связанного с незаконным использованием компьютеров.
Криминологическая характеристика хакерских атак	Криминологическая характеристика хакерской деятельности и других видов компьютерных преступлений. Взаимосвязь компьютерных преступлений с должностной преступностью и коррупцией. Криминологическая характеристика коррупции. Взаимосвязь хакерской деятельности с организованной преступностью. Криминологическая характеристика компьютерной организованной преступности. Взаимосвязь компьютерных мошенничеств с незаконной предпринимательской деятельностью. Криминологическая характеристика незаконной предпринимательской деятельности. *Задание для подготовки:* изучить нормативные правовые акты, касающиеся деятельности, связанной с использованием компьютеров и иной цифровой деятельности; определить место должностной преступности в структуре кибернетической преступности; дать понятие незаконной предпринимательской деятельности; установить взаимосвязь кибернетической преступности с организованной преступностью.
Кибернетическая преступность в зарубежных странах	Общая характеристика кибернетической преступности развитых стран. Общая характеристика кибернетической преступности стран с переходной экономикой. Общая характеристика кибернетической преступности в других странах

	Структура кибернетической преступности за рубежом. Борьба с кибернетической преступностью за рубежом. Соотношение кибернетической и организованной преступности за рубежом. Электронные деньги и компьютерные мошенничества в России и за рубежом: сравнительный анализ. *Задание для подготовки:* изучить нормативные правовые документы, определяющие критерии отнесения одних стран к развитым, а другие страны к странам, с переходной экономикой; изучить и сравнить статистику состояния кибернетической преступности в зарубежных странах; изучить взаимосвязь финансовых преступников и руководителей организованной преступности за рубежом.
Предупреждение кибернетической преступности	Теория предупреждения кибернетической преступности: понятие, признаки и виды. Специальные субъекты предупреждения кибернетической преступности. Методика проведения статистических исследований деятельности, связанной с цифровой экономикой. Методы проведения социологических опросов среди пользователей компьютерными сетями. Криминология интернета. Проведение анонимных опросов и анализ их результатов. Интервью, как средство предупреждения деликтов, правонарушений и преступлений. Граждане, склонные к неоправданному рискованному финансовому поведению: криминологический анализ. *Задание для подготовки:* повторить основы анализа правовой статистики, методику проведения опросов, анкетирования и интервьюирования, изучить методы составления криминологических портретов личности кибер- преступников. Изучить методы проведения интервью, как средства предупреждения правонарушений, связанных с использованием компьютеров и коммуникационных систем. Определить профилактическое значение деятельности специальных подразделений в правоохранительных органах.

2.4. Самостоятельная работа студента

При изучении учебной дисциплины «Кибернетическая преступность» используются следующие виды самостоятельной работы студентов:коллоквиумы, составление анкет, списка вопросов для опросов, документов по предупреждению деликтов, правонарушений, преступлений, криминологических аналитических справок и др. Приведенный минимум может быть расширен за счет использования заданий, дополнительно разработанных в установленном порядке. Указанные виды самостоятельной работы студентов применяются при всех формах обучения.

Примерная тематика заданий:
А) Раскрыть следующие вопросы:

1. Рыночная экономика и преступность: неизбежность и последствия.
2. Теневая экономика и ее влияние на кибернетическую преступность.
3. История кибернетической преступности.

4. Возможности криминологии в обеспечении кибернетической безопасности предпринимательской деятельности.
5. Возможности криминологии в обеспечении кибернетической безопасности обычного человека.
6. Криминологическая характеристика личности кибер-преступников.
7. Криминологическая характеристика личности потерпевших от кибернетических преступлений.
8. Коррупция в компьютерных офисах.
9. Предприниматели и хакеры: точки не соприкосновения.
10. Защита от компьютерных мошенничеств: криминологический отечественный и международный опыт.

Б) Составление процессуальных и иных документов:

1. Вопросы для анкетирования руководителей предприятия, в связи с выявленными компьютерными мошенничествами на предприятии.
2. План опроса потенциальных потерпевших граждан от компьютерных преступлений.
3. Составление аналитической справки по состоянию кибернетической преступности в Москве (ином регионе по указанию преподавателя).
4. Акт о предостережении совершения компьютерных преступлений (по ситуации, предложенной преподавателем).

В) Темы эссе (для заочной формы обучения):

1. Криминология цифрой деятельности.
2. Место криминологического обеспечения кибернетической деятельности в системе наук.
3. Роль юриста в обеспечении безопасности компьютерной деятельности на предприятии, в организации и учреждении.
4. Правовая и моральная статистика: статистические методы выявления компьютерных правонарушений и преступлений.
5. Криминологическая безопасность кадровой политики в области компьютерной деятельность.
6. Компьютерное финансовое мошенничество: криминологические способы выявления и методы противодействия.
7. Криминологическая характеристика кибернетических преступлений: методы противодействия.
8. Взаимосвязь компьютерной преступности и коррупции: непотизм, фаворитизм, а также ее новые элементы.
9. Взаимосвязь кибернетической преступности с организованной преступностью.
10. Теория предупреждения кибернетической преступности.

III. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

В разделе приводятся примерные: а) вопросы для самоконтроля, б) темы рефератов, в) модельные задания. Указанный минимум может быть дополнен за счет использования оценочных средств, разрабатываемых кафедрой в установленном порядке, а также электронных тестовых заданий, имеющихся в централизованной базе данных Университета имени О.Е. Кутафина (МГЮА) в программе http//elearn.msal.ru.

Примерные вопросы для самоконтроля:

1. История кибернетической преступности.
2. Теневая экономика и кибернетическая преступность.
3. Понятие, признаки и виды кибернетической преступности.
4. Тенденции кибернетической преступности.
5. Закономерности кибернетической преступности.
6.Структура и характер кибернетической преступности.
7.Виды латентной кибернетической преступности.
8. Детерминация кибернетической преступности.
9. Классификация причин и условий кибернетической преступности.
10. Социальная обусловленность кибернетической преступности.
11. Влияние личностных факторов на кибернетическую преступность.
12. Понятие и структура личности кибер-преступника.
13. Классификация и типология различных групп и типов компьютерных преступников.
14. Механизм преступного поведения личности кибер-преступника.
15. Виктимологические проблемы кибернетической преступности.
16. Виктимология цифровой экономики.
17.Криминологическая характеристика должностной кибернетической преступности.
18.Причины и условия должностной кибернетической преступности.
19.Криминологическая характеристика взаимосвязи коррупции и кибернетической преступности.
20.Общая характеристика кибернетической преступности за рубежом.
21.Общая характеристика кибернетической преступности в других странах.
22.Соотношение кибернетической и организованной преступности.
23.Взаимосвязь экономических преступников и кибер-преступников.
24. Понятие, признаки и виды предупреждения кибернетической преступности.
25. Специальные субъекты предупреждения кибернетической преступности.
26. Криминология Интернета.

Темы рефератов:

1. Криминологическая характеристика безопасности деятельности, связанной с

коммуникационными системами.
2. Криминологическая характеристика виктимологии кибернетической деятельности.
3. Компьтерные мошенничества на предприятии: способы и методы противодействия.
4. Взаимодействие в вопросах профилактики кибернетической преступности предпринимателей и представителей правоохранительных органов.
5. Современное понятие и состояние коррупции, связанной с коммуникационными системами и меры по противодействию ей.
6. Криминологическая характеристика судебной практики по рассмотрению дел, связанных с кибернетической преступностью.
7. Криминология интернета.
8. Криминология специальных субъектов по борьбе с кибернетическими преступлениями.
9. Криминологическая характеристика компьютерного мошенничества.
10. Специальные субъекты противодействия компьютерной преступности.

Модельные задания:

1. С учетом полученных криминологических знаний разработать максимально защищенную структуру офиса предприятия.
2. Дать криминологическую характеристику законодательства, связанного с компьютерной и другой цифровой деятельностью и уязвимого с криминологической точки зрения,
3. Разработать модель виктимологического безопасного поведения пользователя компьютерами.
4. Составить договор на интернет-обслуживание с гражданином, выделив в нем криминологически значимые элементы.
5. Разработать и представить справку о состоянии кибрнетической преступности за последний год.

IV. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

Нормативно-правовые акты и судебная практика:

1. Конституция Российской Федерации // Российская газета; № 237, 25.12.93Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 N 95-ФЗ // Российская газета, N 137, 27.07.2002
2. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ // Российская газета, N 238-239, 08.12.1994
3. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 N 138-ФЗ // Российская газета, N 220, 20.11.2002
4. Уголовный кодекс Российской Федерации от 13.06.96 № 63- ФЗ // Собрание законодательства РФ; 17.06.96, № 25, ст. 2954

5. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ // Российская газета, N 256, 31.12.2001
6. Трудовой кодекс Российской Федерации от 30.12.2001 N 197- ФЗ // Российская газета , N 256, 31.12.2001
7. Федеральный закон от 12.08.95 N 144-ФЗ "Об оперативно-розыскной деятельности"// Собрание законодательства РФ; 14.08.95, № 33, ст. 3349
8. Федеральный закон от 28.01.2011 № 3-ФЗ «О полиции» // Собрание законодательства РФ; 14.02.2011, № 7, ст. 900.
9. Федеральный закон Российской Федерации «О частной детективной и охранной деятельности в Российской Федерации» от 11.03.92 № 2487-1 // Российская газета, N 100, 30.04.1992.
10. Федеральный закон Российской Федерации от 26.12.95 №208-ФЗ «Об акционерных обществах» // Российская газета , N 248, 29.12.1995
11. Федеральный закон Российской Федерации от 08.02.1998 N 14-ФЗ "Об обществах с ограниченной ответственностью» // Российская газета, N 30, 17.02.1998
12. Федеральный закон Российской Федерации "Об электронной цифровой подписи" от 10.01.2002 N 1-ФЗ // Российская газета, N 6, 12.01.2002
13. Федеральный закон Российской Федерации от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и защите информации» // Российская газета, N 165, 29.07.2006
14. Закон Российской Федерации от 05.03.92 № 2446-1 «О безопасности» // Российская газета, N 103, 06.05.1992
15. Федеральный закон от 23.06.2016 № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» // Собрание законодательства РФ; 27.06.2016, № 26 (Часть I), ст. 3851.
16. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных // Собрание законодательства РФ.2006. № 31 (часть I). Ст. 3451.
17. Федеральный закон от 07.05.2013 № 99-ФЗ «О внесении изменений в отдельные законодательные акты в связи с принятием Федерального закона «О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных» // Собрание законодательства РФ. 2013. № 19. Ст. 2326.
18. Федеральный закон от 23.12.2008 № 294-ФЗ О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля // Собрание законодательства РФ, 29.12.2008, N 52 (ч. 1), ст. 629.
19. Федеральный закон от 7.05.2013 № 78-ФЗ Об уполномоченных по защите прав предпринимателей в Российской Федерации // Собрание законодательства РФ, 13.05.2013 N 19, ст. 2305.
20. Федеральный закон от 17.01.1992 № 2202-1О прокуратуре Российской Федерации // Ведомости СНД РФ и ВС РФ", 20.02.1992, N 8, ст. 366.
21. Федеральный закон от 28.12.201 № 403-ФЗ О Следственном комитете Российской Федерации // Собрание законодательства РФ, 03.01.2011, N 1,

ст. 15.
22. Указ Президента РФ от 09.05.2017 № 203 О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы // Собрание законодательства РФ. 2017. № 20. Ст. 2901.
23. Постановление Правительства РФ от 14.09.2016 N 924 «Об утверждении требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры дорожного хозяйства, требований по обеспечению транспортной безопасности, в том числе требований к антитеррористической защищенности объектов (территорий), учитывающих уровни безопасности для различных категорий объектов транспортной инфраструктуры и транспортных средств автомобильного и городского наземного электрического транспорта, и внесении изменений в Положение о лицензировании перевозок пассажиров автомобильным транспортом, оборудованным для перевозок более 8 человек (за исключением случая, если указанная деятельность осуществляется по заказам либо для собственных нужд юридического лица или индивидуального предпринимателя)» // Собрание законодательства РФ", 26.09.2016, N 39, ст. 5648.
24. Инструкция ЦБ РФ «Об открытии и закрытии банковских счетов по вкладам (депозитам)» от 14.09.06 № 28-И // Вестник Банка России, N 57, 25.10.2006.
25. Постановление Пленума ВАС РФ от 04.04.2014 N 23 "О некоторых вопросах практики применения арбитражными судами законодательства об экспертизе" // URL: http://www.arbitr.ru (дата обращения 10.06.2014).
26. Пленум Верховного Суда РФ от 15 ноября 2016 № 48 О практике применения судами законодательства, регламентирующего особенности уголовной ответственности за преступления в сфере предпринимательской и иной экономической деятельности// Бюллетень Верховного Суда РФ, N 1, январь, 2017.
27. Методические рекомендации по осуществлению прокурорскогонадзора за исполнением законов при расследовании преступлений в сфере компьютерной информации // http://genproc.gov.ru

Основная литература:

1. Мацкевич, И. М. Причины экономической преступности [Электронный ресурс] : учеб. пособие / И. М. Мацкевич ; Моск. гос. юрид. ун-т им.О.Е. Кутафина (МГЮА). - М. : Проспект, 2020. - 272 с. – Режим доступа : http://ebs.prospekt.org/book/34334 (21.08.18).
2. Федоров, А. Ю. Рейдерство и корпоративный шантаж: организаци- онно-правовые меры противодействия : монография / А. Ю. Федоров. - 2-е изд., доп. и перераб. - М. : Юрлитинформ, 2013. - 496 с. + [Элек- тронный ресурс]

2010 г. – Режим доступа :\\consultant\Consultant\cons.exe, локальная сеть МГЮА (21.08.2018).

Дополнительная литература:

1. Антонян Ю.М. Наука криминология. М., Юрлитинформ. 2015.
2. Фукс А. Защита бизнеса от мошенничества. Business School of Owners. М., 2011.
3. Балаян А.Р. Рейдерство в современной России: мошеннические опера-ции с недвижимостью. М., 2009.
4. Барсукова С.Ю. Неформальная экономика. Курс лекций. М., ВШЭ,2009.
5. Безопасность предпринимательской деятельности: Учебник /Под общей редакцией д.ф.н. Шарый Л.Д. – М.: Изд-во «ВК», 2005.
6. Братановский С.Н., Зеленов М.Ф. Административно-правовые аспекты борьбы с коррупцией в системе исполнительной власти в РФ. М., 2020.
7. Варчук Т.В. Виктимология. М., 2009.
8. Ващекин Н.П., Дзлиев М.И., Урсул А.Д. Безопасность предпринимательской деятельности: Учебное пособие. М – ЗАО Изд-во «Экономика», 2002.
9. Волков В. Силовое предпринимательство. Спб., М., 2002.
10. Гамза В.А., Ткачук И.Б. Безопасность коммерческого банка: Учебно-практическое пособие. – М.: Изд-ль Шумилова И.И., 2000
11. Джилад Б. Конкурентная разведка. Изд-во «Питер». М., 2010.
12. Доронин А.И. Формирование корпоративной системы безопасности //Управление корпоративной безопасностью в малом и среднем бизнесе. Высшая школа психологии, М. 2005.
13. Иншаков С.М. Исследование преступности: проблемы методики и методологии. М., 2012.
14. Квалификация коррупционных преступлений в сфере экономики. Учебное пособие. Под ред. А.М. Багмета. М., Юнити-Дана. 2015.
15. Козаченко А.В., Пономарев В.П., Лященко А.Н. Экономическая безопасность предприятия: сущность и механизм обеспечения. Киев, 2003.
16. Королев М.М. Экономическая безопасность фирмы: теория, практика,выбор стратегии. Изд-во «Экономика». М., 2011.
17. Криминология. Учебник для аспирантов. Под ред. И.М. Мацкевич. – М.: Норма, 2017.
18. Криминология. Учебник. Под ред. В.Е. Эминова. М.: Норма. 2015.
19. Лелюхин С.Е., Коротченков А.М., Данилова У.В. Экономическая безопасность в предпринимательской деятельности. М., Проспект. 2016.
20. Социальные отклонения//Кудрявцев В.Н., Бородин С.В., Нерсесянц В.С., Кудрявцев Ю.В. М., Юрид. Лит., 1989.
21. Никонова Н. Г., Добрынин К. Э., Крутильников К. В. Рейдерство: гражданско-правовые и уголовно-правовые аспекты: учебно-методический комплекс. Юридический центр Пресс – 2009.
22. Лопашенко Н.А. Преступления в сфере экономической деятельности.

Части I и II. М., Юрлитинформ. 2015.
23. Лунеев В.В. Истоки и пороки российского уголовного законотворчества. М., Юрлитинформ. 2014.
24. Международно-правовые основы борьбы с коррупцией и отмыванием преступных доходов. Составитель В.С. Овчинский. М, Инфра-М., 2010.
25. Моисеев В.В. Борьба с коррупцией в России. М., Директ-Медия. 2014.
26. Скобликов П.А. Актуальные проблемы борьбы с коррупцией и организованной преступностью в современной России. М., Норма, 2009.
27. Сычев П. Хищники, теория и практика рейдерских захватов. Изд-во «Альпина». М., 2011.
28. Чашин А. Коррупция в России. Стратегия, тактика и методика борьбы. М., 2015.
29. Экономика и организация безопасности хозяйствующих субъектов. Уч- к / Гусев В.С. и др. – СПб.: ИД «Очарованный странник», 2001.
30. Юридическая конфликтология//Отв. Ред. В.Н. Кудрявцев. М., 1995.
31. Ярочкин В.И. Система безопасности фирмы. – 3-е изд., переработ. и доп. – М.: Ось-89, 2003.

Программное обеспечение и электронные ресурсы:

1. СПС «КонсультантПлюс»; Система «ГАРАНТ».
2. www.zonazakona.ru.
3. www.sledovatel.ru;
4. www.crimescience.ru;
5. www.sartraccc.ru;
6. www.yurist.com.

V. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ

1. Аудиторный фонд Университета имени О.Е. Кутафина.
2. Библиотека Университета имени О.Е. Кутафина.
3. Медиатека Университета имени О.Е. Кутафина.
4. Материалы, размещенные на сайте Университета имени О.Е. Кутафина.
5. Аппаратура для дистанционного проектирования.
6. Книги и другие материалы по вопросам криминологии, имеющиеся на кафедре криминологии и уголовно-исполнительного права Университета имени О. Е. Кутафина (МГЮА).
7. НОЦ Криминологический кабинет.