МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

(МОСКОВСКИЙ ПОЛИТЕХ)

Факультет информационных технологий

УТВЕРЖДАЮ

Декан факультета
информационных технологий
/Д. Г. Демидов/

"28" апреля 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Противодействие киберпреступности»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Профиль
«Безопасность открытых информационных систем»

Квалификация
Специалист по защите информации

Формы обучения
Очная

Москва, 2022 г.

Разработчик(и):
Разработчики:
Доцент кафедры «Информационная безопасность», к.т.н, доцент:


/ И.В. Калуцкий /

Согласовано:
И.о. заведующего кафедрой «Информационная безопасность»,


А.Ю. Гневшев

Руководитель образовательной программы,


А.Ю. Гневшев

Содержание

1 Цели, задачи и планируемые результаты обучения по дисциплине

К **основным целям** освоения дисциплины «Противодействие киберпреступности» следует отнести:

- ознакомить с основными понятиями и методами противодействия киберпреступности;
- обеспечить теоретическую и практическую подготовку специалистов к деятельности, связанной с противодействием киберпреступности на локальном, национальном и международном уровнях.

К **основным задачам** освоения дисциплины «Противодействие киберпреступности» следует отнести:

- научить работать с юридической, экономической и иной информацией, относящейся к противодействию киберпреступности;
- привить навыки использования стратегий, техник и методов противодействия киберпреступности в профессиональной деятельности;
- воспитать у обучаемых высокую культуру мышления, т.е. строгость, последовательность, непротиворечивость и основательность в суждениях, в том числе и в повседневной жизни;
- научить понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики;
- привить навыки работы в команде/коллективе, толерантно воспринимая социальные, культурные и иные различия;

развить способности к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия

Обучение по дисциплине **«Противодействие киберпреступности»** направлено на формирование у обучающихся следующих компетенций:

Код и наименование компетенций	Индикаторы достижения компетенции
ОПК—1 – Способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	ИОПК-1.1 Знает основные понятия информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных; ИОПК-1.2. Умеет использовать программные и аппаратные средства персонального компьютера; ИОПК-1.3. Владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).

УК-3 – Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	ИУК-3.1 Понимает цели и задачи команды, свою роль в социальном взаимодействии и командной работе с учетом собственных личных и деловых качеств, интересов команды; владеет основами управления. ИУК-3.2 Реализует свою роль, продуктивно взаимодействуя с другими членами команды ИУК-3.3 Соблюдает правила командной работы; осознает личную ответственность за результаты деятельности и реализацию общекомандных целей и задач
УК-4 – Способность применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1 Обладает знанием основ деловой коммуникации, специфики вербального и невербального взаимодействия, этики делового общения; на должном уровне владеет государственным языком Российской Федерации и необходимым(и) для коммуникации государственным(и) языком субъекта(ов) федерации и иностранным(и) языком (ами) УК-4.2 Осуществляет деловую коммуникацию в устной форме на государственном языке Российской Федерации, государственном(ых) языке(ах) субъекта(ов) федерации и иностранном(ых) языке(ах) с учетом особенностей коммуникаторов и вида делового общения УК-4.3 Осуществляет деловую коммуникацию в письменной форме с использованием официально-делового стиля на государственном языке Российской Федерации, государственном(ых) языке(ах) субъекта(ов) федерации и иностранном(ых) языке(ах), в том числе с учетом правил отечественного делопроизводства и международных норм оформления документов

2 Место дисциплины в структуре образовательной программы

Дисциплина «Противодействие киберпреступности» относится к числу профессиональных учебных дисциплин обязательной части базового цикла (Б1.1) основной образовательной программы специалитета (Б1.2.07), определяемой образовательным учреждением

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ОП: «Управление информационной безопасностью», «Социально-психологические аспекты информационной безопасности».

3 Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 4 зачетных(е) единиц(ы) (144 часа) во втором семестре.

3.1 Виды учебной работы и трудоемкость
(по формам обучения)

3.1.1 Очная форма обучения

№ п/п	Вид учебной работы	Количество часов	Семестры	
			Семестр	Неделя семестра
1	**Аудиторные занятия**	**72**	9	1-18
	В том числе:			
1.1	Лекции		9	1-18
1.2	Семинарские/практические занятия			
1.3	Лабораторные занятия	72	9	2-18
2	**Самостоятельная работа**	**72**	9	2-18
3	**Промежуточная аттестация**			19-21
	Зачет/диф. зачет/экзамен	**Дифференцированный зачет**	9	
	Итого:	**144**		

3.2 Тематический план изучения дисциплины
(по формам обучения)

3.2.1 Очная форма обучения

№ п/п	Разделы/темы дисциплины	Трудоемкость, час					
		Всего	Аудиторная работа				Самостоятельная работа
			Лекции	Семинарские/практические занятия	Лабораторные занятия	Практическая подготовка	
1	Раздел 1. Киберпреступность как особая криминальная угроза						

1.1	Ландшафт угроз кибербезопасности	1					1
1.2	Современный контекст безопасности. Сложность атак.	1					1
1.3	Hi-Tech Crime Trends 2021/2022 как источник стратегической информации о глобальном ландшафте киберугроз и прогнозах их развития.	5			2		1
1.4	Информационная безопасность и преступность.	1					1
1.5	Международное сотрудничество в целях противодействия киберпреступности.	1					1
1.6	Конвенция о киберпреступности (Будапешт, 2001 г.) и дополнительный протокол к ней о типах уголовных правонарушений информационной безопасности.	1					1
1.7	Международные стандарты.	2					2
1.8	Преступления, связанные с применением компьютеров и компьютерных технологий.	4			2		2
1.9	Правовые возможности борьбы с киберпреступностью.	2					2
2	Раздел 2. Киберпреступления и уголовное законодательство Российской Федерации (Глава 28 УК РФ)	1					1
2.1	Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации.	3			2		1
2.2	Преступления в сфере компьютерной информации.	4			2		2
2.3	Иные (общие) преступления, совершаемые с использованием информационных технологий или в отношении телекоммуникационных сетей.	3			2		1
2.4	Квалифицированные составы преступлений.	3			2		1
2.5	Актуальность проблемы обеспечения киберустойчивости Цифровой экономики России в условиях роста угроз безопасности.	4			2		2
2.6	Непрерывность бизнеса как ключевая компонента устойчивости Цифровой экономики России.	1					1
2.7	Уголовная ответственность за киберпреступления по зарубежному уголовному праву. Опыт разных стран.	3			2		1
2.8	Оценка пригодности зарубежного опыта для обеспечения киберустойчивости Цифровой экономики России.	1					1
3	Раздел 3. Обзор основных видов и методов осуществления киберпреступлений						
3.1	Виды и методы киберпреступлений.	4			2		2
3.2	Цели и методы работы современных киберпреступников, обзор практических ситуаций (кейсов).	2					2
3.3	Портрет потенциального злоумышленника. Модель угроз и модель нарушителя	4					4
3.4	Экосистема теневого сегмента сети Интернет. Основные причины роста числа	4			2		2

	киберпреступлений						
3.5	Криптовалюты и анонимные сети.	4			2		2
3.6	Краткий обзор методов сокрытия авторства преступления и способов обналичивания похищенных средств.	2					2
4	Кибербезопасность индустриальных систем.	2			2		
4.1	Защита от утечек через сменные носители. Проблемы на пути внедрения защиты от утечек.	4			2		2
4.2	Проблемы корпоративного управления правами (ERM).	2					2
4.3	Трудности контентной фильтрации.	6			4		2
4.4	Архивирование электронной корреспонденции. Сценарии использования централизованных архивов. Примеры внедрения.	4			2		2
4.5	Новые угрозы безопасности для высокотехнологичных предприятий.	1					1
4.6	Обеспечение киберустойивости информационных систем цифровой индустрии.	1					1
4.7	Киберустойчивость сетей с гибкой типологией.	3			2		1
4.8	Обнаружение инцидентов безопасности в магистральных сетях передачи данных.	6			4		2
4.9	Технологии SIEM для промышленного интернета вещей.	6			4		2
4.10	Создание доверенной среды обмена данными для цифровой индустрии.	1					1
4.11	Тестирование защищенности киберфизических систем.	5			4		1
5	Перспективные технологии и новые вызовы безопасности.	1					1
5.1	Машинное обучение и искусственный интеллект.	1					1
5.2	Автоматизация и роботизация бизнес-процессов.	1					1
5.3	Применение технологии Больших данных в обеспечении кибербезопасности.	7			6		1
5.4	Квантовые вычисления.	1					1
5.5	Новые риски информационной безопасности.	1					1
5.6	Разработка новых технологий для обеспечения киберустойчивости Цифровой экономики России.	1					1
6	Стратегия и тактика противодействия киберпреступности.						
6.1	Стратегии противодействия киберпреступности.	1					1
6.2	Исследования киберугроз, целевых атак и группировок.	5			4		1
6.3	Центры обеспечения безопасности и кибербезопасности.	1					1
6.4	Группа экстренного реагирования на компьютерные инциденты.	1					1
6.5	Расследования высокотехнологичных преступлений	1					1

6.6	Анализ вредоносного кода при расследовании киберпреступлений	4			2		2
6.7	Компьютерная криминалистика.	3			2		1
6.8	Киберучения в формате Red Teaming.	7			6		1
6.9	Комплексный аудит информационной безопасности	6			4		2
Итого		**144**			**72**		**72**

3.3 Содержание дисциплины

Вводная видеолекция

Предмет, цели и задачи курса «Противодействие кибепреступности».

- Предмет, цели и задачи курса.
- Дорожная карта и результат курса.
- Концепция, этапы, содержание учебной работы.

Раздел 1. Киберпреступность как особая криминальная угроза

Ландшафт угроз кибербезопасности (методы и техники атакующих постоянно совершенствуются, злоумышленники используют новые инструменты и векторы атак, которые не детектируются стандартными средствами защиты).

Современный контекст безопасности. Сложность атак.

Hi-Tech Crime Trends 2020/2021 как источник стратегической информации о глобальном ландшафте киберугроз и прогнозах их развития.

Информационная безопасность и преступность. Понятия киберпреступности и киберпреступления. Международные масштабы киберпреступности.

Международное сотрудничество в целях противодействия киберпреступности. Деятельность Интерпола, Европола в борьбе с киберпрступностью.

Конвенция о киберпреступности (Будапешт, 2001 г.) и дополнительный протокол к ней о типах уголовных правонарушений информационной безопасности.

Международные стандарты.

Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконный доступ, получение данных, незаконный перехват информационных ресурсов, искажение информации).

Преступления, связанные с контентом (детская порнография, расизм, агрессивные высказывания и др.).

Преступления, связанные с нарушением интеллектуальных прав.

Преступления, связанные с применением компьютеров и компьютерных технологий (компьютерное мошенничество, использование персональных данных, полученных незаконным путем, кибертерроризм, отмывание денег, др.).

Правовые возможности борьбы с киберпреступностью: обзор международных, региональных и национальных моделей, их взаимосвязь. Господствующие позиции. Спрос на уголовное право. Реалии уголовного права. Проблемы реализации. Субсидиарный характер уголовного права.

Раздел 2. Киберпреступления и уголовное законодательство Российской Федерации (Глава 28 УК РФ)

Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации - Глава 28 Уголовного кодекса Российской Федерации).

Преступления в сфере компьютерной информации. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных компьютерных программ. Нарушение правил эксплуатации средств хранения, обработки или

передачи компьютерной информации и информационно-телекоммуникационных сетей. Описание в законе компьютерной информации как предмета данной группы преступлений. Объективная и субъективная сторона преступлений в сфере компьютерной информации. Квалифицированные виды составов.

Иные (общие) преступления, совершаемые с использованием информационных технологий или в отношении телекоммуникационных сетей, в сфере экономики, охраны конституционных прав граждан, общественной безопасности и здоровья населения. Приемы выделения отдельных преступлений в тексте уголовного закона. Самостоятельные составы преступлений: мошенничество в сфере компьютерной информации. Его особенности.

Квалифицированные составы преступлений (по признакам способа или обстановки совершения): изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних, публичные призывы к осуществлению экстремистской деятельности, публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма и др.

Актуальность проблемы обеспечения киберустойчивости Цифровой экономики России в условиях роста угроз безопасности.

Непрерывность бизнеса как ключевая компонента устойчивости Цифровой экономики России.

Уголовная ответственность за киберпреступления по зарубежному уголовному праву. Опыт разных стран.

Оценка пригодности зарубежного опыта для обеспечения киберустойчивости Цифровой экономики России.

Раздел 3. Обзор основных видов и методов осуществления киберпреступлений

Виды и методы киберпреступлений.

Цели и методы работы современных киберпреступников, обзор практических ситуаций (кейсов).

Портрет потенциального злоумышленника. Модель угроз и модель нарушителя.

Экосистема теневого сегмента сети Интернет. Основные причины роста числа киберпреступлений.

Криптовалюты и анонимные сети.

Основы криптографии.

Краткий обзор методов сокрытия авторства преступления и способов обналичивания похищенных средств.

Раздел 4. Кибербезопасность индустриальных систем

Новые угрозы безопасности для высокотехнологичных предприятий. Эволюция технологий информационной безопасности киберфизических систем с точки зрения теории управления.

Обеспечение киберустойивости информационных систем цифровой индустрии.

Киберустойчивость сетей с гибкой типологией.

Обнаружение инцидентов безопасности в магистральных сетях передачи данных.

Технологии SIEM для промышленного интернета вещей.

Создание доверенной среды обмена данными для цифровой индустрии.

Методология аутентификации в сетях цифровой индустрии.

Тестирование защищенности киберфизических систем.

Раздел 5. Перспективные технологии и новые вызовы безопасности

Машинное обучение и искусственный интеллект.

Автоматизация и роботизация бизнес-процессов.

Применение технологии Больших данных в обеспечении кибербезопасности.

Квантовые вычисления.

Новые риски информационной безопасности.

Разработка новых технологий для обеспечения киберустойчивости Цифровой экономики России.

Раздел 6. Стратегия и тактика противодействия киберпреступности.

Стратегии противодействия киберпреступности.

Исследования киберугроз, целевых атак и группировок.

Центр обеспечения безопасности (Security Operations Center (SOC)).

Центр обеспечения кибербезопасности (Cybersecurity Operations Center (CSOC)).

Группа экстренного реагирования на компьютерные инциденты (Computer Emergency Response Team (CERT).

Коммерческие центры мониторинга и реагирования на компьютерные инциденты (JSOC).

Реагирование на инциденты информационной безопасности. Своевременная идентификация, локализация и ликвидация инцидентов по всему миру.

Использование данных Threat Intelligence & Attribution для восстановления хронологии инцидента и приведения ИТ-инфраструктуру в стабильное состояние в кратчайшие сроки.

Расследования высокотехнологичных преступлений. Борьба с компьютерными, финансовыми, корпоративными преступлениями по всему миру.

Анализ вредоносного кода при расследовании киберпреступлений.

Компьютерная криминалистика, полезные практики, необходимые для обеспечения высокого уровня кибербезопасности.

Киберучения в формате Red Teaming. Имитация целевых атак и регулярное противодействие им.

Комплексный аудит информационной безопасности (современный контекст безопасности. требует принципиально нового подхода к проведению аудита; оценки только технической оснащенности уже недостаточно для гарантии готовности к сложным атакам). Полный цикл проверок для всестороннего аудита инфраструктуры и оценки защищенности компании от сложных киберугроз.

Технологии

- Отсутствие следов компрометации (ретроспективно) и критических уязвимостей
- Надежные средства защиты инфраструктур

Процессы

- Подробное журналирование событий
- Полнота, актуальность и практическое применение регламентов реагирования

Люди

- Компетентность всех членов команды реагирования
- Осведомленность сотрудников о киберугрозах

Аудит на предмет внешних угроз

- Проверка готовности команды ИБ к реагированию для оценки работы действующих в компании регламентов
- Внешнее тестирование на проникновение для проверки защищенности инфраструктуры от внешних атак и проникновения злоумышленников во внутреннюю сеть компании
- Социоинженерное тестирование для оценки осведомленности сотрудников о киберугрозах

Аудит на предмет внутренних угроз

- Диагностика компрометации инфраструктуры для раскрытия готовящихся атак

- Внутреннее тестирование на проникновение для оценки готовности к атаке от нарушителя, имеющего доступ к локальной сети

Комплекс методов для досконального исследования сети на предмет уязвимостей и компрометации, оценки готовности к реагированию и возможности воздействия на сотрудников методами социальной инженерии.

Правила цифровой гигиены в условиях удаленной работы.

Ключевые правила по безопасному выходу из режима удаленной работы.

Анализ практических ситуаций.

3.4 Тематика семинарских/практических и лабораторных занятий

Семинарские/практические занятия в учебном плане не запланированы.

3.4.2 Лабораторные занятия

Лабораторная работа 1 «Изучение Hi-Tech Crime Trends»

Лабораторная работа 2. «Анализ преступлений, связанных с применением компьютеров и компьютерных технологий».

Лабораторная работа 3. «Уголовная ответственность за совершение киберпреступлений (преступлений в сфере компьютерной информации».

Лабораторная работа 4. «Преступления в сфере компьютерной информации».

Лабораторная работа 5. «Преступления, совершаемые с использованием информационных технологий или в отношении телекоммуникационных сетей».

Лабораторная работа 6. «Квалифицирование состава преступлений».

Лабораторная работа 7. «Обзор актуальным проблем киберустойчивости цифровой экономики».

Лабораторная работа 8. «Виды и методы киберпреступлений».

Лабораторная работа 9. «Анализ экосистемы теневого сегмента сети Интернет».

Лабораторная работа 10. «Криптовалюты и блок-чейны».

Лабораторная работа 11. «Кибербезопасность индустриальных систем».

Лабораторная работа 12. «Защита от утечек через сменные носители».

Лабораторная работа 13. «Фильтрация и блокировка контента в сети».

Лабораторная работа 14. «Сценарии использования централизованных архивов».

Лабораторная работа 15. «Контентная фильтрация».

Лабораторная работа 16. «Архивирование электронной корреспонденции».

Лабораторная работа 17. Киберустойчивость сетей с гибкой типологией.

Лабораторная работа 18. Обнаружение инцидентов безопасности в магистральных сетях передачи данных.

Лабораторная работа 19. Технологии SIEM для промышленного интернета вещей.

Лабораторная работа 20. Тестирование защищенности киберфизических систем.

Лабораторная работа 21. Применение технологии Больших данных в обеспечении кибербезопасности.

Лабораторная работа 22. Исследования киберугроз, целевых атак и группировок.

Лабораторная работа 23. Анализ вредоносного кода при расследовании киберпреступлений.

Лабораторная работа 24. Киберучения в формате Red Teaming.

Лабораторная работа 25. Комплексный аудит информационной безопасности.

3.5 Тематика курсовых проектов (курсовых работ)

Учебным планом курсовое проектирование не предусмотрено.

4 Учебно-методическое и информационное обеспечение

4.1 Нормативные документы и ГОСТы

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) // Российская газета. № 237. 25.12.1993.
2. Гражданский кодекс Российской Федерации (Часть первая) от 30 ноября 1994 года N 51-ФЗ
3. Гражданский кодекс Российской Федерации (Часть вторая) от 26.01.1996 № 14-ФЗ // СЗ РФ. 1996. № 5. ст. 410.
4. Гражданский кодекс Российской Федерации часть 3 (ГК РФ ч.3) от 26 ноября 2001 года N 146-ФЗ
5. Гражданский кодекс Российской Федерации часть 4 (ГК РФ ч.4) от 18.12.2006 № 230-ФЗ
6. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // СЗ РФ. 1996. № 25. ст. 2954.
7. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. I).ст. 4921.
8. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ // Российская газета. № 256., 31.12.2001.

9. Гражданский кодекс Российской Федерации (Часть четвертая) от 18.12.2006 № 230-ФЗ // СЗ РФ. 2006. № 52 (1 ч.).ст. 5496.

10. Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» // СЗ РФ. 1997. № 41. стр. 8220-8235.

11. Федеральный закон от 02.12.1990 № 395-1 «О банках и банковской деятельности» // СЗ РФ.1996. № 6. ст. 492.

12. Федеральный закон от 07.08.2001 № 119-ФЗ «Об аудиторской деятельности» // СЗ РФ. 2001. № 33 (часть I).ст. 3422.

13. Федеральный закон от 10.01.2002 № 1-ФЗ «Об электронной подписи» // СЗ РФ. 2002. № 2. ст. 127.

14. Федеральный закон "О лицензировании отдельных видов деятельности" от 04.05.2011 N 99-ФЗ

15. Федеральный закон "О техническом регулировании" от 27.12.2002 N 184-ФЗ

16. Федеральный закон от 07.07.2003 № 126-ФЗ «О связи» // СЗ РФ. 2003. № 28. ст. 2895.

17. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне» // СЗ РФ. 2004. № 32. ст. 3283.

18. Федеральный закон от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

19. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3448.

20. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» // СЗ РФ. 2006. № 31 (1 ч.).ст. 3451.

21. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"

22. Указ Президента РФ от 20.01.1996 N 71 "Вопросы Межведомственной комиссии по защите государственной тайны"

23. Указ Президента РФ от 16.08.2004 N 1085 "Вопросы Федеральной службы по техническому и экспортному контролю"

24. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»

25. Федеральный закон "О федеральной службе безопасности" от 03.04.1995 N 40-ФЗ

26. Федеральный закон от 31.05.1996 N 61-ФЗ «Об обороне»

27. Указ Президента РФ от 06.03.1997 N 188 "Об утверждении Перечня сведений конфиденциального характера"

28. Указ Президента РФ от 01.05.2022 N 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации"

29. Постановление Правительства РФ от 03.11.1994 N 1233 "Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»

30. Постановление Правительства Российской Федерации от 3 февраля 2012 г. N 79 «О лицензировании деятельности по технической защите конфиденциальной информации»

31. Постановление Правительства Российской Федерации от 3 марта 2012 г. N 171 О лицензировании деятельности по разработке и производству средств защиты конфиденциальной информации

32. Постановление Правительства РФ от 02.06.2008 N 418 "О Министерстве

цифрового развития, связи и массовых коммуникаций Российской Федерации"

33. Постановление Правительства РФ от 15.04.1995 N 333 (ред. от 03.02.2023) "О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны"

34. Постановление Правительства РФ от 06.02.2010 N 63 (ред. от 10.07.2020) "Об утверждении Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне"

35. Постановление Правительства РФ от 26.06.1995 N 608 (ред. от 21.04.2010) "О сертификации средств защиты информации"

36. Постановление Правительства РФ от 15.07.2022 N 1272 "Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)"

37. Приказ ФСБ РФ от 24.10.2022 № 524 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств"

38. Приказ ФСБ России от 10.07.2014 N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности"

39. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

40. Приказ ФСТЭК России от 29 апреля 2021 г. N 77 «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»

41. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»

42. Приказ ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

43. Приказ ФСТЭК России от 23 марта 2017 г. N 49 «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. n 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному

контролю от 14 марта 2014 г. n 31»

44. Приказ ФСТЭК России от 03.04.2018 N 55 (ред. от 19.09.2022) "Об утверждении Положения о системе сертификации средств защиты информации"

45. "Методический документ. Методика оценки угроз безопасности информации" (утв. ФСТЭК России 05.02.2021)

46. ГОСТ Р 53131-2008 «Защита информации. Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий. Общие положения».

47. ГОСТ Р ИСО/МЭК 27005-2010 Национальный стандарт российской федерации информационная технология методы и средства обеспечения безопасности менеджмент риска информационной безопасности

48. "ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования"

49. ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности»

4.2 Основная литература

1. Криулин, А. А. Основы безопасности прикладных информационных технологий и систем : учебное пособие / А. А. Криулин, В. С. Нефедов, С. И. Смирнов. — Москва : РТУ МИРЭА, 2020. — 136 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/167606.
2. Нефедов, В. С. Основы обеспечения анонимности в сети Интернет : учебное пособие / В. С. Нефедов, А. А. Криулин, Г. Ю. Потерпеев. — Москва : РТУ МИРЭА, 2022. — 81 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/240041
3. Информационная безопасность и защита информации в цифровой экономике элементы теории и тестовые задания : учебное пособие / И. Д. Алекперов, В. В. Храмов, А. А. Горбачева, Д. С. Фомичев. — Ростов-на-Дону : ИУБиП, 2020. — 114 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/248747
4. Петренко, В. И. Защита персональных данных в информационных системах. Практикум : учебное пособие для СПО / В. И. Петренко, И. В. Мандрица. 2-е изд., стер. - Санкт-Петербург: Лань, 2022. 108 с. – ISBN 978-5-8114-9038-7 — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/183744

4.3 Дополнительная литература

1. Кибербезопасность цифровой индустрии. Теория и практика устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.

2. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны /пер. с англ. Д.А. – М.: ДМК Пресс, 2020. – 326 с.: ил.
3. Петренко С. Киберустойчивость цифровой экономики. Как обеспечить безопасность и непрерывность бизнеса. – СПб: Питер, 2021. – 384 с.: ил.
4. Сафронов Е.В. Азы кибергигиены: методологические и правовые аспекты. – Москва, Проспект, 2021. – 48 с.
5. Всестороннее исследование проблемы киберпреступности https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf.
6. Шелупанов А.А., Смолина А.Р. Форензика. Теория и практика расследования киберпреступлений. – М.: Горячая линия – Телеком. 2020. – 104 с.: ил.
7. Кибербезопасность цифровой индустрии. Теория и практика устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия – Телеком, 2020. – 560 с.: ил.
8. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны /пер. с англ. Д.А. – М.: ДМК Пресс, 2020. – 326 с.: ил.
9. Петренко С. Киберустойчивость цифровой экономики. Как обеспечить безопасность и непрерывность бизнеса. – СПб: Питер, 2021. – 384 с.: ил.
10. Сафронов Е.В. Азы кибергигиены: методологические и правовые аспекты. – Москва, Проспект, 2021. – 48 с.
11. Всестороннее исследование проблемы киберпреступности https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Russian.pdf.
12. Шелупанов А.А., Смолина А.Р. Форензика. Теория и практика расследования киберпреступлений. – М.: Горячая линия – Телеком. 2020. – 104 с.: ил.
13. Suzanne Widup. Computer Forensics and Digital Investigation with EnCase Forensic v7 (Networking & Communication - OMG). 2014;
14. Brett Shavers, John Bair. Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis. 2016.

4.4 Электронные образовательные ресурсы

1. Электронный образовательный ресурс разрабатывается.
2. Московский Политех подключен к ЭБС: Юрайт, АйПиАр и Лань
3. https://mospolytech.ru/obuchauschimsya/biblioteka/
4. -Банк данных угроз безопасности информации (доступно по ссылке: https://bdu.fstec.ru/);
5. Информационное сообщение о разработке методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» от 9 апреля 2020 г. № 240/22/1534

4.5 Лицензионное и свободно распространяемое программное обеспечение

Для выполнения лабораторных работ и самостоятельной работы необходимо следующее программное обеспечение:

1. Microsoft Windows.
2. Веб-браузер, Chrome.

4.6 Современные профессиональные базы данных и информационные справочные системы

6. Справочная правовая система "КонсультантПлюс" https://www.consultant.ru/
7. Официальный сайт ФСТЭК России https://fstec.ru/
8. Образовательная платформа *«Юрайт»* https://urait.ru/

5 Материально-техническое обеспечение

И лекционные и лабораторные занятия могут проводится дистанционно в формате онлайн. Преподавателю для проведения занятий необходим ноутбук с возможностью использования сервиса корпоративной платформы Microsoft Teams или других платформ для проведения занятий, например, Zoom. У студентов должна быть возможность выхода в Интернет.

6 Методические рекомендации

6.1 Методические рекомендации для преподавателя по организации обучения

При подготовке к занятиям следует предварительно проработать материал занятия, предусмотрев его подачу точно в отведенное для этого время занятия. Следует подготовить необходимые материалы – теоретические сведения, задачи и др. При проведении занятия следует контролировать подачу материала и решение заданий с учетом учебного времени, отведенного для занятия.

При проверке работ и отчетов следует учитывать не только правильность выполнения заданий, но и оптимальность выбранных методов решения, правильность выполнения всех его шагов.

6.2 Методические указания для обучающихся по освоению дисциплины

Самостоятельная работа студентов помогает получить дополнительные теоретические и практические знаниями по изучаемой дисциплине, развивает сознательное отношение к интеллектуальному труду.

В процессе самостоятельной работы, студенты дорабатывают конспекты лекций, готовятся к дифференцированному зачету, изучают рекомендованную литературу, осуществляют подборку нормативно-правовых документов и проводят ознакомительный анализ с ними, готовятся к лабораторным работам, выполняют домашние задания;

Самостоятельная работа позволяет закрепить и углубить знания, полученные во время аудиторных занятий, а также изучить отдельные темы учебной программы.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;

- контроль со стороны преподавателей (текущий и промежуточный).

Лекционные занятия дают общее представление по изучаемой теме, основной знания студент получает в процессе выполнения лабораторных работ и самостоятельной работы.

Практические занятия проводятся по наиболее важным темам дисциплины. Осуществляется закрепление знаний, полученных студентами на лекциях и в процессе самостоятельной работы. Особое внимание обращается на развитие умений и навыков установления связи положений теории с профессиональной деятельностью будущего специалиста по ИБ. *Написание лабораторных работ* предполагает более детальное изучение нормативно-правовых документов, регламентирующих деятельность по защите информации, в рамках определённой тематики, а также обмен мнениями по поставленным *вопросам,* в процессе разбора проверенных работ.

Домашним заданием, по большей части, является подготовка к следующей лабораторной работе. Студентам предлагается выполнить подбор литературы, нормативно-правовых документов, по тематике лабораторной работы, и предварительное ознакомление с ними.

При проведении лабораторной работы преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, отвечает на вопросы студентов, проверяет выполненные работы. На следующем занятии, подводится итог проведенной работы, студентам сообщаются результаты, ведется обсуждение рассмотренных вопросов подводится итог занятию в целом.

По результатам выполнения всех видов учебной работы, предусмотренных учебным планом (подготовка конспектов лекций, успешное выполнение лабораторных работ, подготовка домашнего задания, присутствие и активная работа на занятиях) по данной дисциплине (модулю), преподаватель может рассмотреть возможность проставления положительной оценки на дифференцированном зачете «Автоматом», при этом учитываются результаты текущего контроля успеваемости в течение семестра. В случае, если студент длительно отсутствовал на занятиях, не выполнял задания он всё равно допускается до дифференцированного зачета, но на дифференцированном зачете, таким студентам, преподаватель может задавать любое количество вопросов по всем темам данной дисциплины (в рамках отведённого времени), дабы убедиться, что студент самостоятельно освоил дисциплину.

Текущий контроль осуществляется на практических занятиях, промежуточный контроль осуществляется на зачёте в письменной (устной) форме.

7 Фонд оценочных средств

7.1 Методы контроля и оценивания результатов обучения

В процессе обучения используются следующие оценочные формы самостоятельной работы студентов, оценочные средства текущего контроля успеваемости и промежуточных аттестаций:

- домашние задания и их защита;
- лабораторные работы,
- дифференцированный зачет.

7.2 Шкала и критерии оценивания результатов обучения

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю)

ОПК-1. Способность оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**
знать: основные понятия информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных	Обучающийся демонстрирует полное отсутствие знаний основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных.	Обучающийся демонстрирует неполное соответствие знаний основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	Обучающийся демонстрирует частичное соответствие следующих знаний: основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	Обучающийся демонстрирует полное соответствие следующих знаний: основных понятий информатики, назначение, функции и структуру операционных систем, вычислительных сетей и систем управления базами данных, свободно оперирует приобре-тенными знаниями.
уметь: - Умеет использовать программные и аппаратные средства персонального компьютера;	Обучающийся не умеет или в недостаточной степени умеет использовать программные и аппаратные средства персонального компьютера.	Обучающийся демонстрирует неполное соответствие следующих умений: применять программные и аппаратные средства персонального компьютера. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: применять программные и аппаратные средства персонального компьютера. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие следующих умений: применять программные и аппаратные средства персонального компьютера. Свободно оперирует приобретенными умениями, применяет их в ситуациях

				повышенной сложности.
владеть: - навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).	Обучающийся не владеет или в недостаточной степени владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).	Обучающийся владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.)., допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.).. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениям и (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т.п.)., свободно применяет полученные навыки в ситуациях повышенной сложности.
УК-3 Способность организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели;				
Знает: цели и задачи команды, свою роль в социальном взаимодействии и командной работе с учетом собственных личных и деловых качеств, интересов	Обучающийся не знает: цели и задачи команды, свою роль в социальном взаимодействии и командной работе с учетом собственных личных и деловых качеств, интересов команды; владеет основами управления	Обучающийся демонстрирует неполное знание: целей и задач команды, свою роль в социальном взаимодействии и командной работе с учетом собственных личных и деловых качеств, интересов команды; владеет основами управления. Допускаются значительные ошибки, проявляется недостаточность знаний, по	Обучающийся демонстрирует частичное знание целей и задач команды, свою роль в социальном взаимодействии и командной работе с учетом собственных личных и деловых	Обучающийся демонстрирует знание: целей и задач команды, свою роль в социальном взаимодействии и командной работе с учетом собственных личных и

команды; владеет основами управления		ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	качеств, интересов команды; владеет основами управления. Допускаются незначительные ошибки, неточности, затруднения при аналитических операциях.	деловых качеств, интересов команды; владеет основами управления. Свободно оперирует приобретёнными знаниями.
Умеет: реализовать свою роль, продуктивно взаимодействуя с другими членами команды.	Обучающийся не умеет: реализовать свою роль, продуктивно взаимодействуя с другими членами команды.	Обучающийся демонстрирует неполное соответствие следующих умений: реализовать свою роль, продуктивно взаимодействуя с другими членами команды. Допускаются значительные ошибки, проявляется недостаточность умений.	Обучающийся демонстрирует частичное соответствие следующих умений: - реализовать свою роль, продуктивно взаимодействуя с другими членами команды. Умения освоены, но допускаются незначительные ошибки, неточности.	Обучающийся демонстрирует полное соответствие умений: реализовать свою роль, продуктивно взаимодействуя с другими членами команды. Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
Владеет: - навыками соблюдения правил командной работы; осознает личную ответственность за результаты деятельности и реализацию общекомандных целей и задач.	Обучающийся не владеет: - навыками соблюдения правил командной работы; не осознает личную ответственность за результаты деятельности и реализацию общекомандных целей и задач..	Обучающийся владеет - навыками соблюдения правил командной работы; осознает личную ответственность за результаты деятельности и реализацию общекомандных целей и задач., но допускаются значительные ошибки, проявляется недостаточность владения навыками.	Обучающийся частично владеет - навыками соблюдения правил командной работы; осознает личную ответственность за результаты деятельности и реализацию общекомандных целей и задач. Навыки освоены, но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет - навыками соблюдения правил командной работы; осознает личную ответственность за результаты деятельности и реализацию общекомандных целей и задач..

Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: дифференцированный зачёт

Промежуточная аттестация обучающихся, в форме дифференцированного зачета, проводится по результатам выполнения всех видов учебной работы, предусмотренных учебным планом по данной дисциплине (модулю), при этом учитываются результаты текущего контроля успеваемости в течение семестра. Оценка степени достижения обучающимися планируемых результатов обучения по дисциплине (модулю) проводится преподавателем, ведущим занятия по дисциплине (модулю) методом экспертной оценки. По итогам промежуточной аттестации по дисциплине (модулю) выставляется оценка «отлично», «хорошо», «удовлетворительно» или «неудовлетворительно».

Шкала оценивания	Описание
Отлично	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателей, оперирует приобретенными знаниями, умениями, навыками, применяет их в ситуациях повышенной сложности. При этом могут быть допущены незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.
Хорошо	Выполнены все виды учебной работы, предусмотренные учебным планом. Студент демонстрирует неполное, правильное соответствие знаний, умений, навыков приведенным в таблицах показателей, либо если при этом были допущены 2-3 несущественные ошибки.
Удовлетворительно	Студент демонстрирует соответствие знаний, в котором освещена основная, наиболее важная часть материала, но при этом допущена одна значительная ошибка или неточность.
Неудовлетворительно	Не выполнен один или более видов учебной работы, предусмотренных учебным планом. Студент демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускаются значительные ошибки, проявляется отсутствие знаний, умений, навыков по ряду показателей, студент испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

7.3 Оценочные средства

7.3.1 Примерный список вопросов для дифференцированного зачета

1) Информационная безопасность и преступность. Понятия киберпреступности и киберпреступления
2) Формы противодействия киберпреступности.
3) Нормативно-правовые основы информационной безопасности в Российской Федерации
4) Международное сотрудничество в области защиты информации, противодействия киберпреступности.

5) Правовые стратегии борьбы с киберпреступностью: обзор международных, региональных и национальных моделей, их взаимосвязь
6) Киберпреступления в системе Особенной части УК РФ
7) Преступления в сфере компьютерной информации: характеристика составов
8) Уголовная ответственность за киберпреступления в зарубежных странах
9) Типичные способы совершения киберпреступлений
10) Методы сокрытия авторства преступления в сети Интернет
11) Атрибуция кибератак. Понятие источника действий в сети Интернет. Методы атрибуции источника кибератак
12) Понятие доказательств в цифровом виде. Источники сбора доказательств в цифровом виде.
13) Методы компьютерно-технических экспертиз, их правовые основы.
14) Расследование киберпреступлений. Государственные органы, осуществляющие расследование киберпреступлений. Международное сотрудничество в расследовании киберпреступлений.
15) Машинное обучение и искусственный интеллект: новые риски информационной безопасности.

Пример билета.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(МОСКОВСКИЙ ПОЛИТЕХ)

Курс «Противодействие киберпреступности»

Зачет

Билет №__

1. Информационная безопасность и преступность. Понятия киберпреступности и киберпреступления.
2. Правовые стратегии борьбы с киберпреступностью: обзор международных, региональных и национальных моделей, их взаимосвязь