МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДЕНО
Декан факультета
Информационных технологий
_____ / А.Ю. Филиппович /
«28» мая 2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Противодействие киберпреступности»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

Образовательная программа (профиль)
«Обеспечение информационной безопасности распределенных информационных систем»

Квалификация (степень) выпускника
Специалист по защите информации

Очная
Год приема - 2020

Москва 2020 г.

1. Цели освоения дисциплины.

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, в том числе в сфере профессиональной деятельности.

2. Место дисциплины в структуре ООП.

Дисциплина «Противодействие киберпреступности» относится к числу профессиональных учебных базовой части цикла (Б.1) основной образовательной программы (Б.1.48).

Изучение дисциплины опирается на знания, умения и навыки, приобретенные в предшествующих дисциплинах: «Основы коммуникации», «Основы информационной безопасности», «Криптографические методы защиты информации», «Аудит информационной безопасности», «Безопасность сетей электронных вычислительных машин», «Безопасность систем баз данных», «Защита конфиденциальной информации и персональных данных».

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенные с планируемыми результатами освоения образовательной программы.

В результате освоения дисциплины (модуля) у обучающихся формируются следующие компетенции и должны быть достигнуты следующие результаты обучения как этап формирования соответствующих компетенций:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать	Перечень планируемых результатов обучения по дисциплине
ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику **уметь:** выступать с презентациями по вопросам профессиональной деятельности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	**Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата; **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды.
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	**Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно- коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках; - использовать диалогическое общение для сотрудничества в академической коммуникации общения: • внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям; • уважая высказывания других как в плане содержания, так и в плане формы; • критикуя аргументированно и конструктивно, не задевая чувств других; • адаптируя речь и язык жестов к ситуациям

		взаимодействия. **Владеть:** навыками выполнять перевод профессиональных текстов с иностранного (-ых) на государственный язык и обратно.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 4 зачетных единицы, т.е. **144** академических часов (лекции- 36 часов, лабораторные занятия – 36 час, самостоятельная работа - 72 часов, форма контроля – зачет) в 8 семестре.

Структура и содержание дисциплины «Противодействие киберпреступности» по срокам и видам работы отражены в приложении.

Содержание разделов 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.

Тема № 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.

Тема № 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.

Тема № 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.

Тема 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.

Тема № 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.

Тема 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.

5. Образовательные технологии.

Методика преподавания дисциплины «Противодействие киберпреступности» и реализация компетентностного подхода в изложении и восприятии материала предусматривает использование следующих активных и интерактивных форм проведения групповых, индивидуальных, аудиторных занятий в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков обучающихся:

- подготовка к выполнению лабораторных работ;

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 70 % аудиторных занятий.

6. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины и учебно-методическое обеспечение самостоятельной работы студентов.

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

- компьютерное тестирование;
- зачет.

Образцы тестовых заданий, экзаменационных билетов, приведены в приложении.

6.1. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине (модулю).

6.1.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы.

В результате освоения дисциплины (модуля) формируются следующие компетенции:

Код компетенции	В результате освоения образовательной программы обучающийся должен обладать
ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства
УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде
УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)

В процессе освоения образовательной программы данные компетенции, в том числе их отдельные компоненты, формируются поэтапно в ходе освоения обучающимися дисциплин (модулей), практик в соответствии с учебным планом и календарным графиком учебного процесса.

6.1.2. Описание показателей и критериев оценивания компетенций, формируемых по итогам освоения дисциплины (модуля), описание шкал оценивания

Показателем оценивания компетенций на различных этапах их формирования является достижение обучающимися планируемых результатов обучения по дисциплине (модулю):
Шкалы оценивания результатов промежуточной аттестации и их описание:

Форма промежуточной аттестации: экзамен.

Промежуточная аттестация обучающихся в форме экзамена 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	Выполнены все виды учебной работы, предусмотренные учебным планом. 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 показателей, 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.

Фонды оценочных средств представлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная 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.

Перечень основных нормативных документов

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ (УК РФ) (с изменениями и дополнениями). Глава 28. Преступления в сфере компьютерной информации.
2. Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изменениями и дополнениями).
3. Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных» (с изменениями и дополнениями).
4. Федеральный закон от 26 июля 2006 г. N 135-ФЗ «О защите конкуренции» (с изменениями и дополнениями).
5. Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (с изменениями и дополнениями)

6. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне» (с изменениями и дополнениями).
7. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Международные стандарты

1. Конвенция против киберпреступности (СДСЕ 185-2001).
2. Будапештская конвенция.
3. Дополнительный протокол к Дополнительному протоколу к Конвенции о киберпреступности (СДСЕ 189) (далее - Конвенция).
4. ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements.
5. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements.

б) дополнительная литература:

1. Global Cybersecurity Index. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
2. Новые технологии противодействия киберпреступности: по материалам круглых столов «Международный опыт использования цифровых технологий в борьбе с киберпреступностью» и «Блокчейн технологии и противодействие кибертерроизма»): [Электронный ресурс]: / Текст. дан. и граф. – М.: Изд. «Научный консультант», 2019.
3. Антонян Е.А., Аминов И.И. Блокчейн-технологии в противодействии кибертерроризму // Актуальные проблемы российского права, №6 (103), 2019. – 167 – 177.
4. Кончена А. Реальные опасности виртуального мира: есть ли защита от киберпреступлений? [Электронный ресурс]. URL: https://rb.ru/opinion/virtual-world/.
5. Иван Мелехин «Киберпреступность выходит на профессиональный уровень». [Электронный ресурс]. URL: https://plus.rbc.ru/news/5fe9d57a7a8aa9473122f54b?utm_source=rbc&utm_medium=main&utm_campaign=830949-5fe9d57a7a8aa9473122f54b
6. Об итогах голосования в Генассамблее ООН по российскому проекту резолюции по противодействию киберпреступности [Электронный ресурс]. URL: https://www.mid.ru/ru/organs/-/asset_publisher/AfvTBPbEYay2/content/id/3988579
7. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С.М. Корабельников. – Москва : Издательство Юрайт, 2020. – 111 с. – (Высшее образование).
8. Чернова Е.В. Информационная безопасность человека. Учебное пособие для вузов. Издательство Юрайт. Москва, 2020. – 243 с.
9. Kali Linux. Тестирование на проникновение и безопасность. – Питер, 2020.
10. Сбер и BI.ZONE приняли участие в ежегодном саммите по вопросам кибербезопасности Всемирного экономического форума [Электронный ресурс]. URL: https://www.sberbank.com/ru/news-and-media/press-releases/article?newsID=c99781b9-edf7-43e5-a5e0-5c8f6f1086ef&blockID=7&regionID=77&lang=ru&type=NEWS
11. Group-IB и JSOC запускают совместный сервис по предотвращению киберпреступлений [Электронный ресурс]. URL: https://www.group-ib.ru/media/jsoc-solar/

12. Розенцвайг А.И., Чертилин В.С. Формы противодействия киберпреступности// Вестник экономики, права и социологии, 2019, № 4. [Электронный ресурс]. URL: http://www.vestnykeps.ru/0419/30.pdf
13. AUTOMATED COMPLIANCE & CYBER SECURITY SOLUTIONS Электронный ресурс]. URL: https://varpath.com/
14. Герке М. Понимание киберпреступности: явление, задачи и законодательный ответ/ http://www.itn.int/ITUD/cyb/cybersecurity/legislation.html
15. Suzanne Widup. Computer Forensics and Digital Investigation with EnCase Forensic v7 (Networking & Communication - OMG). 2014;
16. Brett Shavers, John Bair. Hiding Behind the Keyboard: Uncovering Covert Communication Methods with Forensic Analysis. 2016.
17. Machine learning in Computer Forensics https://pralab.diee.unica.it/sites/default/files/Ariu_AISEC2011.pdf
18. Квантовые компьютеры и конец безопасности https://blog.kaspersky.ru/kvantovye-kompyuteryi-konec-bezopasnosti/1989/

в) программное обеспечение и интернет-ресурсы:

Hi-Tech Crime Trends 2020/2021

Программное обеспечение: Word, Excel, PowerPoint, программное обеспечение для просмотра видео- и аудиоконтента и др.

Интернет-ресурсы:

- Банк данных угроз безопасности информации (доступно по ссылке: https://bdu.fstec.ru/);

- Информационное сообщение о разработке методического документа ФСТЭК России «Методика определения угроз безопасности информации в информационных системах» от 9 апреля 2020 г. № 240/22/1534

https://fstec.ru/component/attachments/download/2728

https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy

- Проект методического документа «Методика моделирования угроз безопасности информации»

https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/149-proekty/2070-metodicheskij-dokument

Для успешного освоения дисциплины студенту рекомендуется использовать следующие программные средства:

1. Автоматизированная информационно-поисковая правовая система «КонсультантПлюс»;
2. Автоматизированная информационно-поисковая правовая система «Гарант»;
3. Автоматизированная информационно-поисковая правовая система «Lexis-Nexis»

8. Материально-техническое обеспечение дисциплины.

Для проведения всех видов занятий необходимо презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

1. Операционная система Windows 7 или более поздней версии или аналог.
2. Microsoft Office XP или более поздней версии или аналог.
3. Антивирусное ПО «Kaspersky Antivirus» 7.0 или более поздней версии или аналог.

Для проведения лабораторных занятий необходимо наличие компьютерных классов, оборудованных современной вычислительной техникой из расчета одно рабочее место на одного обучаемого.

Система LMS.

Оборудование и аппаратура.

1 презентационное оборудование (мультимедийный проектор, экран) – 1 комплект.

Персональный компьютер (из расчета 1 оборудованное рабочее место на одного обучаемого).

Компьютерный класс с доступом к сети Интернет.

1. Веб-браузер Chrome.
2. Microsoft Visual Studio.
3. Microsoft Office.

9. Методические рекомендации для самостоятельной работы студентов

Изучение дисциплины осуществляется в строгом соответствии с целевой установкой в тесной взаимосвязи учебным планом. Основой теоретической подготовки студентов являются лекции.

В процессе самостоятельной работы студенты закрепляют и углубляют знания, полученные во время аудиторных занятий, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

10. Методические рекомендации для преподавателя

Программа составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки б **10.05.03 «Информационная безопасность автоматизированных систем»**.

Программу составил: Темникова К.Н.

Программа утверждена на заседании кафедры “Информационная

безопасность” «28» мая 2020 г., протокол № 1

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Приложение.

Структура и содержание дисциплины «Противодействие киберпреступности»
по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»
(специалист)

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов					Формы аттестации	
				Л	П/С	Лаб	СРС	КСР	К.Р.	К.П.	ДЗ	Реферат	К/р	Э	З
	8 семестр														
1	Тема № 1. Киберпреступность как особая криминальная угроза (Часть 1)	8	1	2		2	4								
2	Тема № 1. Киберпреступность как особая криминальная угроза (Часть 2)		2	2		2	4								
3	Тема № 1. Киберпреступность как особая криминальная угроза (Часть 3)		3	2		2	4								
4	Тема № 2. Киберпреступления и уголовное законодательство Российской Федерации (Глава 28 УК РФ) (Часть 1)		4	2		2	4								
5	Тема № 2. Киберпреступления и уголовное законодательство Российской Федерации (Глава 28 УК		5	2		2	4								

	РФ) (Часть 2)															
6	Тема № 2. Киберпреступления и уголовное законодательство Российской Федерации (Глава 28 УК РФ) (Часть 3)		6	2		2	4									
7	Тема № 3. Обзор основных видов и методов осуществления киберпреступлений (Часть 1)		7	2		2	4									
8	Тема № 3. Обзор основных видов и методов осуществления киберпреступлений (Часть 2)		8	2		2	4									
9	Тема № 3. Обзор основных видов и методов осуществления киберпреступлений (Часть 3)		9	2		2	4									
10	Тема 4. Кибербезопасность индустриальных систем (Часть 1)		10	2		2	4									
11	Тема 4. Кибербезопасность индустриальных систем (Часть 2)		11	2		2	4									
12	Тема 4. Кибербезопасность индустриальных систем (Часть 3)		12	2		2	4									
13	Тема № 5. Перспективные технологии и новые вызовы безопасности (Часть 1)		13	2		2	4									
14	Тема № 5. Перспективные технологии и новые вызовы безопасности (Часть 2)		14	2		2	4									
15	Тема № 5. Перспективные технологии и новые вызовы безопасности (Часть 3)		15	2		2	4									
16	Тема 6. Стратегия и тактика		16	2		2	4									

	противодействия киберпреступности (Часть 1)														
17	Тема 6. Стратегия и тактика противодействия киберпреступности (Часть 2)		17	2		2	4								
18	Тема 6. Стратегия и тактика противодействия киберпреступности (Часть 3)		18	2		2	4								
	Форма аттестации	8	19-21							.					З
	Всего часов по дисциплине в 8 семестре			36		36	72								
	Всего часов по дисциплине			36		36	72								

Приложение к
рабочей программе

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

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем» ОП (профиль): «Обеспечение информационной безопасности распределенных информационных систем»

Форма обучения: очная

Вид профессиональной деятельности: эксплуатационная; проектно-технологическая; экспериментально-исследовательская; организационно-управленческая

Кафедра: «Информационная безопасность»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ

«Противодействие киберпреступности»

Состав: 1. Паспорт фонда оценочных средств
2. Описание оценочных средств:
Компьютерное тестирование
Зачет

Составители: доц. Темникова К.Н.

Москва, 2020 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Противодействие киберпреступности					
ФГОС ВО **10.05.03 «Информационная безопасность автоматизированных систем»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **общепрофессиональные и профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетен**	**Форма оценоч-ного**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				

ОПК—1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	**знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику **уметь:** выступать с презентациями по вопросам профессиональной деятельности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики	Лекции, самостоятельная работа, лабораторные занятия	КТ, Зачет	Базовый уровень: **знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику **уметь:** выступать с презентациями по вопросам профессиональной деятельности **владеть:** высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики Повышенный уровень: **знать:** основные нормативные правовые акты в области информационной безопасности, профессиональную этику, лучшие практики деловых коммуникаций **уметь:** выступать с презентациями по вопросам профессиональной деятельности, в том числе при внедрении систем менеджмента информационной безопасности, системы менеджмента непрерывности деятельности **владеть:** навыками формирования системы финансовой и нефинансовой мотивации к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики

УК-3	Способен осуществлять социальное взаимодействие и реализовывать свою роль в команде	**Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата; **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды.	Лекции, самостоятельная работа, лабораторные занятия	КТ, Зачет	Базовый уровень: **Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата; **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды. Повышенный уровень: **Знать:** - эффективность использования стратегии сотрудничества для достижения поставленной цели, определяет свою роль в команде; - особенности поведения выделенных групп людей, с которыми работает/взаимодействует, учитывать их в своей деятельности; **Уметь:** моделировать ситуации, прогнозировать результаты (последствия) личных действий и планировать последовательность шагов для достижения заданного результата при внедрении систем менеджмента информационной безопасности, системы менеджмента непрерывности деятельности **Владеть:** навыками эффективного взаимодействия с другими членами команды, в т.ч. навыками участия в обмене информацией, знаниями и опытом, и приемами эффективной презентации результатов работы команды

УК-4	Способен осуществлять деловую коммуникацию в устной и письменной формах на государственном языке Российской Федерации и иностранном(ых) языке(ах)	**Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно- коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках; - использовать диалогическое общение для сотрудничества в академической коммуникации общения: • внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям; • уважая высказывания других как в плане содержания, так и в плане формы; • критикуя аргументированно и конструктивно, не задевая чувств других; • адаптируя речь и язык жестов к ситуациям взаимодействия. **Владеть:** навыками выполнять перевод профессиональных текстов с иностранного (-ых) на государственный язык и обратно.	Лекции, самостоятельная работа, лабораторные занятия	КТ, Зачет	Базовый уровень: **Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно-коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках; - использовать диалогическое общение для сотрудничества в академической коммуникации общения: **Владеть:** навыками выполнять перевод профессиональных текстов с иностранного (-ых) на государственный язык и обратно. Повышенный уровень: **Знать:** подходы к выбору на государственном и иностранном (-ых) языках коммуникативно приемлемых стилей делового общения, вербальных и невербальных средств взаимодействия с партнерами; **Уметь:** - использовать информационно- коммуникационные технологии при поиске необходимой информации в процессе решения стандартных коммуникативных задач на государственном и иностранном (- ых) языках; - вести деловую переписку, учитывая особенности стилистики официальных и неофициальных писем, социокультурные различия в формате корреспонденции на государственном и иностранном (-ых) языках; - использовать диалогическое общение для сотрудничества в академической коммуникации общения: • внимательно слушая и пытаясь понять суть идей других, даже если они противоречат собственным воззрениям; • уважая высказывания других как в плане

Приложение 2
к рабочей программе

Оценочные средства для текущей аттестации

Компьютерное тестирование

Промежуточное тестирование

По каждой теме предлагается 10 вопросов для тестирования в системе LMS. Освоение темы зависит от результата написания теста: 9-10 баллов – тема считается освоенной на продвинутом уровне; 6-8 баллов – тема считается освоенной на базовом уровне; 0-5 баллов – тема считается не освоенной. В тесте представлены задания/вопросы разных типов. Тест содержит вопросы по материалам теории и пройденных лабораторных работ.

Тесты представлены в системе LMS.

Итоговое тестирование

Итоговый тест включает 70% промежуточных тестов, сформированных на основе случайного выбора из всего банка тестовых заданий/вопросов для промежуточного тестирования и 30% тестовых заданий/вопросов, отличных от промежуточных, то есть не вошедших в промежуточные тесты заданий/вопросов.

Тесты представлены в системе LMS.

Оценочные средства для промежуточной аттестации

Зачет

Зачет принимается либо в виде итогового теста в системе LMS, либо в устной форме при ответе на вопросы билета. В билете содержится 2 (два) вопроса.

Список вопросов для зачета по дисциплине

Примерный перечень вопросов для итогового 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 БЮДЖЕТНОЕ 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