МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«МОСКОВСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ

Декан факультета информационных технологий

Филиппович А.Ю.

"01" сентября 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«Методы коммуникаций в области информационной безопасности»

Направление подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

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

Квалификация (степень) выпускника
Специалист

Форма обучения
Очная
Год приема - 2019

Москва 2019 г.

1. Цели освоения дисциплины.

К **основным целям** освоения дисциплины «Методы коммуникаций в области информационной безопасности» следует отнести:

- теоретическая и практическая подготовка специалистов в области информационной безопасности в части определения потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться коммуникации.

К **основным задачам** освоения дисциплины «Методы коммуникаций в области информационной безопасности» следует отнести:

- овладение методами и формами коммуникаций в области информационной безопасности.

2. Место дисциплины в структуре ООП.

Дисциплина «Методы коммуникаций в области информационной безопасности» относится к числу профессиональных учебных дисциплин базовой части Б.1.1 (Б.1.1.17) основной образовательной программы специалитета.

Дисциплина взаимосвязана логически и содержательно-методически со следующими дисциплинами и практиками ООП: «Основы информационной безопасности», «Разработка технических текстов и документации», «Аудит безопасности конфиденциальных и персональных данных», «Навыки эффективной презентации».

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**
ОК-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	**Знать** методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности. **Уметь** определять потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда

		обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться коммуникации; планировать внешние и внешние коммуникации компании по вопросам информационной безопасности. **Владеть** методами эффективной коммуникации в процессе постановки задач и оценки рисков информационной безопасности.

4. Структура и содержание дисциплины.

Общая трудоемкость дисциплины составляет 2 зачетных единицы, т.е. 72 академических часа (лабораторные занятия - 36 часов, самостоятельная работа – 36 часов, форма контроля - зачет) в 3 семестре.

Структура и содержание дисциплины «Методы коммуникаций в области информационной безопасности» по срокам и видам работы отражены в приложении.

Содержание разделов дисциплины

3 семестр

Тема 1. Методы и формы коммуникаций в области информационной безопасности

Коммуникации и их значение в системе управления. Коммуникации относительно соблюдения правил информационной безопасности. Методы коммуникации, используемые для обеспечения информационной безопасности – состояния информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования и т.п. Основные этапы и элементы коммуникационного процесса. Коммуникационные сети, их виды.

Методы коммуникации в организациях. Управление связями с общественностью как внешний метод общения организации. Внутренние методы коммуникаций и их характеристики. Международные коммуникации.

Анализ коммуникативного процесса и его элементов в организации. Организационно-экономическая характеристика предприятия. Анализ этапов коммуникационного процесса в организации. Основные направления совершенствования коммуникационного процесса в организации.

Планирование внешних и внешних коммуникаций компании по вопросам информационной безопасности. Участники коммуникаций, их целеполагание и мотивация. Скорость получения информации и отклика. Понятие эффективных коммуникаций. Виды отношений по степени регламентированности. Коммуникационная стратегия.

Коммуникации в подразделении информационной безопасности. Взаимодействие начальника отдела информационной безопасности и его подчиненных. Основные подходы к построению эффективных коммуникаций и распределению обязанностей.

Коммуникации подразделения информационной безопасности с другими подразделениями предприятия. Методы коммуникаций, используемых при решении вопросов выявления уязвимостей, развития кадрового потенциала подразделения информационной безопасности, охраны труда, бюджетирования. приобретения/замены оборудования в целях повышения уровня информационной безопасности и иных практических вопросов.

Особенности коммуникаций в случае несанкционированного доступа к информационным ресурсам предприятия (хакерских атак). Методы коммуникаций, которые используют специалисты по защите информации, хакеры и социальные инженеры. Проблемы информационной и коммуникационной приватности, этичности поведения в Интернете, интеллектуальной собственности, профессиональной этики и ответственности ИТ-специалистов. Рассматриваются этические ситуации, связанные с несанкционированным копированием личных данных, злоупотреблением информацией, созданием персональных «досье». Инциденты проблемного поведения в Интернете, случаи хищения и вымогательства в киберпространстве.

Тема 2. Правовое регулирование коммуникаций в области информационной безопасности

Информация как объект правовой защиты. Правовое регулирование коммуникаций в области информационной безопасности. Государственная система обеспечения информационной безопасности Российской Федерации.

Методы коммуникации, способствующие организации работы коллектива исполнителей в профессиональной деятельности с учетом требований законодательства, регулирующих органов, контрактных обязательств.

Особенности применения методов коммуникации в области информационной безопасности в рамках реализации Федерального закона от 27.07.2006 N 149-ФЗ (с изм. и доп.) "Об информации, информационных технологиях и о защите информации".

Особенности применения методов коммуникации в области информационной безопасности в рамках реализации Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Особенности применения методов коммуникации в области информационной безопасности в рамках реализации Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".

Особенности применения методов коммуникации в области информационной безопасности в рамках реализации Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 31.12.2017) "О персональных данных".

Особенности применения методов коммуникации в области информационной безопасности в рамках реализации Федерального закона от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) "О коммерческой тайне".

Особенности применения методов коммуникации в области информационной безопасности в банковской сфере.

Особенности применения методов коммуникации в области информационной безопасности при использовании электронного документооборота.

Тема 3. Коммуникации в процессе обучения работников предприятия по вопросам информационной безопасности

Необходимость обучения работников предприятия по вопросам информационной безопасности. Методы коммуникаций и действия, приводящие к незаконному овладению конфиденциальной информацией.

Взаимодействие работников подразделения информационной безопасности с руководством предприятия и другими подразделениями предприятия по вопросам выбора форм и методов обучения (в форме лекций, обучающих презентаций, обучающих видеороликов, плакатов и иных наглядных материалов, игрофикация обучения), тестирования, повторного тестирования, личных бесед.

Тестирование сотрудников организации. Проверка навыков сотрудников (рассылка фейковых акций)

Применение методов коммуникации при обучении и повышении осведомленности сотрудников в области информационной безопасности (периодически со всеми сотрудниками; единоразово и затем периодически - с новоприбывшими сотрудниками).

Формирование коммуникационной стратегии предприятия в области информационной безопасности. Развитие коммуникаций при разработке и внедрении парольной политики предприятия, политики размещения информации работниками предприятия в социальных сетях.

Тема 4. Применение методов коммуникации при формировании и развитии системы менеджмента информационной безопасности

Применение методов коммуникации в процессе управления информационной безопасностью, построении системы менеджмента информационной безопасности (СМИБ), определении потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться коммуникации.

Важность коммуникаций в контексте ISO 27001-2013, ИСО 27001, ГОСТ Р ИСО/МЭК 27001-2006 и ГОСТ Р ИСО/МЭК 27002-2012.

Эффективные коммуникации в области информационной безопасности при использовании преимущества стандарта ISO/IEC 27001: (1) возможность выявления рисков и принятия мер по их оптимизации или устранению; (2) гибкость адаптации инструментов к любым областям вашей деятельности; (3) доверие со стороны заинтересованных лиц и клиентов благодаря защите их данных ; (4) соответствие стандартам гарантирует статус привилегированного поставщика; (5) удовлетворение любых ожиданий благодаря соответствию требованиям стандартов.

Применение методов коммуникации в процессе постановки задач и оценки рисков информационной безопасности.

5. Образовательные технологии.

Методика преподавания дисциплины «Методы коммуникаций в области информационной безопасности» 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 практических работ с использованием видео уроков;
- проведение интерактивных лекционных и практических занятий в форме видео уроков;
- проведение групповых упражнений;
- обсуждение и защита домашних заданий по дисциплине;
- подготовка, представление и обсуждение презентаций на семинарских занятиях.

Удельный вес занятий, проводимых в интерактивных формах по дисциплине, составляет 60 % аудиторных занятий. Занятия лекционного типа составляют 33 % от объема 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:

- подготовка к решению прикладных задач, групповых упражнений;
- зачет.

Образцы тестовых заданий, заданий для проектной работы студентов, контрольных вопросов и заданий для проведения текущего контроля, билетов для зачета, 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
ОК-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия

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:

ОК-6 способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия				
Показатель	**Критерии оценивания**			
	2	**3**	**4**	**5**

знать: методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности.	Обучающийся демонстрирует полное отсутствие или недостаточное соответствие следующих знаний: методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности.	Обучающийся демонстрирует неполное соответствие следующих знаний: методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности. Допускаются значительные ошибки, проявляется недостаточность знаний, по ряду показателей, обучающийся испытывает значительные затруднения при оперировании знаниями при их переносе на новые ситуации.	методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности.	Обучающийся демонстрирует полное соответствие следующих знаний: методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности. ,свободно оперирует приобретенными знаниями.
определять потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться коммуникации; планировать внешние и внешние коммуникации	Обучающийся не умеет или в недостаточной степени умеет определять потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться	Обучающийся демонстрирует неполное соответствие следующих умений: определять потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться коммуникации; планировать внешние и внешние коммуникации компании по вопросам	Обучающийся демонстрирует частичное соответствие следующих умений: определять потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны	Обучающийся демонстрирует полное соответствие следующих умений: определять потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться

компании по вопросам информационной безопасности.	коммуникации; планировать внешние и внешние коммуникации компании по вопросам информационной безопасности.	информационной безопасности. . Допускаются значительные ошибки, проявляется недостаточность умений.	осуществляться коммуникации; планировать внешние и внешние коммуникации компании по вопросам информационной безопасности.. Умения освоены, но допускаются незначительные ошибки, неточности.	коммуникации; планировать внешние и внешние коммуникации компании по вопросам информационной безопасности. . Свободно оперирует приобретенными умениями, применяет их в ситуациях повышенной сложности.
владеть: методами эффективной коммуникации в процессе постановки задач и оценки рисков информационной безопасности.	Обучающийся не владеет или в недостаточной степени владеет методами эффективной коммуникации в процессе постановки задач и оценки рисков информационной безопасности.	Обучающийся владеет, допускаются значительные ошибки, методами эффективной коммуникации в процессе постановки задач и оценки рисков информационной безопасности. , проявляется недостаточность владения навыками.	Обучающийся частично владеет методами эффективной коммуникации в процессе постановки задач и оценки рисков информационной безопасности. , но допускаются незначительные ошибки, неточности, затруднения.	Обучающийся в полном объеме владеет методами эффективной коммуникации в процессе постановки задач и оценки рисков информационной безопасности. , свободно применяет полученные навыки в ситуациях повышенной сложности.

Форма промежуточной аттестации: зачет.

Промежуточная аттестация обучающихся в форме 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.

Шкала оценивания	**Описание**
Зачтено	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.

Не зачтено	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 средствпредставлены в приложении к рабочей программе.

7. Учебно-методическое и информационное обеспечение дисциплины.

а) основная литература:

1. Федеральный закон от 27.07.2006 N 149-ФЗ (с изм. и доп.) "Об информации, информационных технологиях и о защите информации".
2. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".
3. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации".
4. ISO 27001-2013.
5. Кияев В., Граничин О. Безопасность информационных систем: курс. Национальный Открытый Университет «ИНТУИТ» 2016 г.
6. Нестеров С. А. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ. Учебник и практикум для СПО. Научная школа: Санкт-Петербургский политехнический университет Петра Великого (г. Санкт-Петербург). Год: 2018 / Гриф УМО СПО

б) дополнительная литература:

1. Родичев Ю. Информационная безопасность: нормативно-правовые аспекты: Учебное пособие. 2007.
2. Защита и обработка конфиденциальных документов: практикум. СКФУ 2016 г.
3. Минин И. В., Минин О. В. Защита конфиденциальной информации при электронном документообороте: учебное пособие. НГТУ 2011 г.
4. Конфиденциальное делопроизводство и защищенный электронный документооборот: учебник. Логос. 2011 г.
5. Лапина М. А., Говорова С. В., Пелешенко В. С. Менеджмент инцидентов информационной безопасности защищенных автоматизированных систем управления: учебное пособие. СКФУ 2017 г.
6. Загинайлов Ю. Н. Теория информационной безопасности и методология защиты информации: учебное пособие. Директ-Медиа. 2015 год
7. Малюк Анатолий Александрович. Этика в сфере информационных технологий / А.А. Малюк, О.Ю. Полянская, И.Ю. Алексеева. - М.: Гор. линия-Телеком, 2011. ISBN 978-5-9912-0197-1
8. Ратников, В. П. Деловые коммуникации : учебник для бакалавров / В. П. Ратников ; отв. ред. В. П. Ратников. — М. : Издательство Юрайт, 2015. — 527 с. — (Серия : Бакалавр. Академический курс). — ISBN 978-5-9916-3685-8.
9. Жернакова, М. Б. Деловые коммуникации : учебник и практикум для прикладного бакалавриата / М. Б. Жернакова, И. А. Румянцева. — М. : Издательство Юрайт, 2018. — 370 с. — (Серия : Бакалавр. Прикладной курс). — ISBN 978-5-534-00331-4.

в) программное обеспечение и интернет-ресурсы:

1. Журнал «Защита информации. Инсайд». Сайт журнала – http://www.inside-zi.ru/

2. Журнал «Безопасность информационных технологий». Сайт журнала – сайт журнала http://www.pvti.ru/articles_14.htm.
3. Журнал «Информация и безопасность». Сайт журнала – http://kafedrasib.ru/?page_id=119.
4. Журнал «Information Security/Информационная безопасность». Издатель: компания «Гротек». Сайт журнала – http://www.itsec.ru.
5. ЭБС издательства Лань – http://e.lanbook.com/.
6. Научная электронная библиотека eLIBRARY.RU – http://elibrary.ru/.
7. Библиографическая и реферативная база данных научной периодики «Scopus» - www.scopus.com.
8. Сайт Федеральной службы безопасности России (ФСБ России). -http://www.fsb.ru.
9. Информационно-аналитический Интернет-портал ISO27000.ru. – http://www.iso27000.ru/
10. Портал по безопасности. – http://www.sec.ru/.
11. Локальный электронный учебник по направлению «Информационная безопасность» для бакалавров и специалистов. Федоров Н.В. Свидетельство о государственной регистрации программы для ЭВМ № 2013610300.
12. Операционная система Windows 7(или ниже) – MicrosoftOpenLicense Лицензия № 61984214, 61984216,61984217, 61984219, 61984213, 61984218, 61984215.
13. Офисные приложения, MicrosoftOffice 2013(или ниже) – MicrosoftOpenLicense Лицензия № 61984042.

8. Материально-техническое обеспечение дисциплины.

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

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

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, дорабатывают конспекты лекций, готовятся к экзамену, а также самостоятельно изучают отдельные темы учебной программы.

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. *Практические занятия* проводятся по теоретическим и проблемным вопросам ИБ. Практическое занятие предполагает творческие дискуссии, активный обмен мнениями по поставленным *вопросам,* заслушивание и обсуждение докладов по предложенным преподавателем темам.

Важным обстоятельством является привлечение внимания студентов к обсуждаемой проблеме, стимулирование интереса к ней и организация активного обсуждения, как структуры проблемы, так и составляющих ее наиболее актуальных тем. Для повышения эффективности проведения занятия требуется предварительная

подготовка всех его участников. В этой связи рекомендуется заблаговременно (не менее, чем за неделю) оповестить студентов о теме занятия, дать перечень литературы по теме, назначить из числа студентов докладчиков и содокладчиков.

При проведении практического занятия преподаватель *выполняет, в основном,* функции ведущего - следит за регламентом времени, помогает уточнить формулировки, обобщает результаты дискуссии, подводит итог занятию в целом. При высоком уровне подготовки студенческой группы отдельные функции ведущего можно поручить одному из студентов. В случае необходимости, преподаватель оказывает ему поддержку, а при подведении итогов - дает оценку работе ведущего.

Активная работа студента на практическом занятии учитывается при определении итоговой оценки его знаний по дисциплине на зачете.

Самостоятельная работа по дисциплине предполагает: выполнение студентами домашних заданий. Домашние задания являются, как правило, продолжением практических занятий и содействуют овладению практическими навыками по основным разделам дисциплины. Самостоятельная работа студентов предполагает изучение теоретического и практического материала по актуальным вопросам дисциплины. Рекомендуется самостоятельное изучение учебной и научной литературы, использование справочной литературы и др.

При выдаче заданий на самостоятельную работу используется дифференцированный подход к студентам. Перед выполнением студентами самостоятельной внеаудиторной работы преподаватель проводит инструктаж по выполнению задания, который включает: цель здания, его содержание, сроки выполнения, ориентировочный объем работы, основные требования к результатам работы, критерии оценки. В процессе инструктажа преподаватель предупреждает студентов о возможных типичных ошибках, встречающихся при выполнении задания. Инструктаж проводится преподавателем за счет объема времени, отведенного на изучение дисциплины.

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

Самостоятельная работа осуществляется индивидуально.

Контроль самостоятельной работы организуется в двух формах:

- самоконтроль и самооценка студента;
- контроль со стороны преподавателей (текущий и промежуточный).

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

Критериями оценки результатов самостоятельной работы студента являются:

- уровень освоения студентом учебного материала;
- умения студента использовать теоретические знания при выполнении практических задач;
- сформированность компетенций;
- оформление материала в соответствии с требованиями.

10. Методические рекомендации для преподавателя

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

Программу составил: доцент, к.э.н. К.Н. Темникова.

Программа утверждена на заседании кафедры “Информационная безопасность” «29» августа 2019 г., протокол № 1.

Заведующий кафедрой
«Информационная безопасность»

к.т.н., доцент Н.В. Федоров

Структура и содержание дисциплины «Методы коммуникаций в области информационной безопасности» по направлению подготовки
10.05.03 «Информационная безопасность автоматизированных систем»

n/n	Раздел	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов, и трудоемкость в часах					Виды самостоятельной работы студентов	Формы аттестации		
				Л	ПЗ	Лаб	СРС	КСР	К.П. К.Р. ДЗ Реферат	К/р	Э	З
1	Методы и формы коммуникаций в области информационной безопасности	3	**1**			2	2					
2			**2**			2	2					
3			**3**			2	2					
4			**4**			2	2					
5	Правовое регулирование коммуникаций в области информационной безопасности		**5**			2	2					
6			**6**			2	2					
7			**7**			2	2					
8			**8**			2	2					
9	Коммуникации в процессе обучения работников предприятия по вопросам информационной безопасности		**9**			2	2					
10			**10**			2	2					
11			**11**			2	2					
12			**12**			2	2					
13	Применение методов коммуникации при формировании и развитии системы менеджмента информационной безопасности		**13**			2	2					
14			**14**			2	2					
15			**15**			2	2					
16			**16**			2	2					

17			**17**			2	2					
18	Защита прикладной задачи (проекта)		**18**			2	2					
	Форма аттестации		**19-21**									**З**
	Всего часов по дисциплине в третьем семестре					36	36					

Приложение

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

«Методы коммуникаций в области информационной безопасности»

Состав: 1. Паспорт фонда оценочных средств

2. Описание оценочных средств:

Самостоятельные работы
Зачет

Составители: доцент, к.э.н. Темникова К.Н.

Москва, 2019 год

Таблица 1

ПОКАЗАТЕЛЬ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ

Безопасность компьютерных систем (кибербезопасность новой информационной среды)					
ФГОС ВО **10.03.01 «Информационная безопасность»**					
В процессе освоения данной дисциплины студент формирует и демонстрирует следующие **профессиональные компетенции**:					
КОМПЕТЕНЦИИ		**Перечень компонентов**	**Технология формирования компетенций**	**Форма оценоч-ного средств**	**Степени уровней освоения компетенций**
ИН-ДЕКС	**ФОРМУЛИРОВКА**				
ОК-6	способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия	**Знать** методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности. **Уметь** определять потребности организации во внутренних и внешних коммуникациях, существенных для функционирования системы менеджмента информационной безопасности, включая: a) на какой предмет обмениваться информацией, b) когда обмениваться информацией; c) с кем обмениваться информацией; d) кто должен обмениваться информацией; и e) процессы, посредством которых должны осуществляться коммуникации; планировать внешние и внешние коммуникации компании по	лекции, самостоятельная работа, практические занятия	СР зачет	Базовый уровень: демонстрирует полное соответствие следующих знаний: методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности Повышенный уровень: демонстрирует полное соответствие следующих знаний: методы и формы коммуникаций в области информационной безопасности, правовое регулирование коммуникаций в области информационной безопасности в условиях повышенной сложности, свободно оперирует приобретенными знаниями.

Оценочные средства для текущей аттестации

Прикладная задача (проект)

«Определение наиболее эффективных методов коммуникации в области информационной безопасности для идентификации рисков предприятия «АВС»

Дано: Предприятие «АВС» создано на территории Российской Федерации в 2010 году. На предприятии работает 250 человек. Сфера деятельности – производство датчиков. Режим коммерческой тайны на предприятии не введен. В течение ближайших двух лет предприятие планирует расширить сферу деятельности и осуществлять разработку и производство промышленных контроллеров и датчиков, программного обеспечения для систем автоматизации и диспетчеризации промышленных и жилищно-коммунальных объектов. Предприятие является финансово-устойчивым, количество заказов ежегодно увеличивается. В ближайшие два года планируется увеличение количества работников предприятия «АВС» на 20%, ввести режим коммерческой тайны. Собственником предприятия поставлена задача повысить уровень информационной безопасности, используя наиболее эффективные методы коммуникации.
Специалисту по информационной безопасности, который работает на предприятии «АВС», известны следующие стратегии хакеров
Стратегия 1.
Использование промежутков времени между выявлением уязвимостей и установкой соответствующих обновлений.
Стратегия 2.
Обман пользователей при помощи методов социального инжиниринга.
Стратегия 3.
Внедрение вредоносного программного обеспечения (ПО) в предположительно безвредный контент, например, в рекламные объявления.
Известно также, что:
- хакеры придумывают все новые способы распространения вредоносного ПО;
- появляется новая тенденция по использованию вымогательского программного обеспечения (ПО) не с целью финансовой выгоды, а для сокрытия истинных мотивов киберпреступных действий;
- средний возраст злоумышленника снижается за счет использования вредоносного ПО, как сервиса;
- злоумышленники часто эксплуатируют такие чувства как *любопытство, жадность* и др. Для проведения своих атак злоумышленники, применяющие техники социальной инженерии, зачастую эксплуатируют *доверчивость, лень, любезность* и даже *энтузиазм* пользователей и сотрудников организаций. Защититься от таких атак непросто, поскольку их жертвы могут не подозревать, что их обманули.

Вопросы:

1. Назовите методы и формы коммуникации, которые позволят обеспечить защиту информационного потока предприятия «АВС».
2. Какую информацию должен анализировать специалист по информационной безопасности, директор департамента по информационной безопасности для принятия управленческого решения по используемым методам коммуникации?
3. Приведите примеры из практики, подтверждающие основные стратегии хакеров и тенденции атак: массовые атаки; атаки на поставщиков и контрагентов; APT-атаки (целевые атаки); атаки в сфере «Интернет вещей (IoT)»; атаки в сфере «майнинг». Каким образом этот опыт может применить специалист по информационной

безопасности, который работает на предприятии «АВС»? Какие методы коммуникации в области информационной безопасности наиболее эффективны для идентификации рисков предприятия «АВС»?

4. Какие особенности применения методов коммуникации возникают в случае, если на предприятии «АВС» вводится режим коммерческой тайны?
5. Какие особенности применения методов коммуникации возникают в случае, если предприятие «АВС» обязано выполнять требования Федерального закона от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации"?
6. Составьте перечень наиболее эффективных методов коммуникации в области информационной безопасности для предприятия «АВС» с учетом перспектив развития предприятия.

Источники:

1. Федеральный закон от 27.07.2006 N 149-ФЗ (с изм. и доп.) "Об информации, информационных технологиях и о защите информации".
2. Федеральный закон от 26.07.2017 N 187-ФЗ "О безопасности критической информационной инфраструктуры Российской Федерации".
3. Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 18.04.2018) "О коммерческой тайне".
4. Cisco. Годовой отчет по информационной безопасности, 2017г.
5. Cisco. Годовой отчет по информационной безопасности, 2018г.
6. Positive Technologies. Актуальные киберугрозы. IV квартал 2017 г.
7. Positive Technologies. Актуальные киберугрозы. 2017-2018: цифры, факты, прогнозы.
8. Отчет PandaLabs. 2017 г.

Оценочные средства для промежуточной аттестации

Зачет

Список вопросов для зачета по дисциплине

Вопросы к зачету

по курсу

«**Методы коммуникаций в области информационной безопасности**»

1. Коммуникации в области информационной безопасности: основные методы.
2. Методы коммуникации в области информационной безопасности и их применение при планировании внешних и внутренних коммуникаций, постановке задач и оценке рисков.
3. Формы коммуникации в области информационной безопасности.
4. Методы коммуникации в области информационной безопасности и их применение при взаимодействии с банками. Программа «Клиент-Банк».

5. Методы коммуникации в области информационной безопасности и их применение при использовании физическими лицами on-line банка.
6. Методы коммуникации в области информационной безопасности и их применение при взаимодействии с инвесторами.
7. Методы коммуникации в области информационной безопасности и их применение при взаимодействии с деловыми партнерами (поставщиками).
8. Методы коммуникации в области информационной безопасности и их применение при взаимодействии с деловыми партнерами (потребителями)
9. Методы коммуникации в области информационной безопасности и их применение при взаимодействии с деловыми партнерами (страховыми компаниями).
10. Методы коммуникации в области информационной безопасности и их применение при использовании на предприятии режима коммерческой тайны, особенности передачи и обработки информации.
11. Методы коммуникации в области информационной безопасности и их применение при заключении соглашения о неразглашении (конфиденциальности).
12. Методы коммуникации в области информационной безопасности и их применение при использовании персональных данных. Особенности передачи и обработки персональных данных.
13. Методы коммуникации в области информационной безопасности и их применение при необходимости применить санкции за разглашение коммерческой тайны.
14. Методы коммуникации в области информационной безопасности и их применение при необходимости применить санкции за разглашение персональных данных.
15. Методы коммуникации в области информационной безопасности и их применение при использовании электронного документооборота (ЭДО).
16. Методы коммуникации в области информационной безопасности и их применение при обучении персонала по вопросам информационной безопасности.
17. Методы коммуникации в области информационной безопасности и их применение при использовании социальных сетей.
18. Методы коммуникации, применяемые при хакерской атаке.
19. Методы коммуникации, применяемые при взаимодействии с «социальным инженером».
20. Методы коммуникаций, применяемые для повышения эффективности защиты от действий хакеров и социальных инженеров.
21. Применение методов коммуникации на различных этапах построения системы информационной безопасности.
22. Применение методов коммуникации в случае нападения на политику безопасности и процедуры административного доступа.
23. Применение методов коммуникации в случае нападения на постоянные компоненты системы защиты.
24. Применение методов коммуникации в случае нападения на сменные элементы системы защиты.
25. Применение методов коммуникации в случае нападения на протоколы информационного взаимодействия.
26. Применение методов коммуникации в случае нападения на функциональные элементы компьютерных сетей.

Пример билета.

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

Курс «Методы коммуникаций в области информационной безопасности»

Зачет

Билет №__

Вопросы:

1. Коммуникации в области информационной безопасности: основные методы.
2. Методы коммуникации в области информационной безопасности и их применение при планировании внешних и внутренних коммуникаций, постановке задач и оценке рисков.
3. Прикладная задача.