Федеральное государственное бюджетное образовательное учреждение высшего образования
«ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ ДВАЖДЫ ГЕРОЯ СОВЕТСКОГО СОЮЗА, ЛЕТЧИКА-КОСМОНАВТА А.А. ЛЕОНОВА»

Троицкий Александр Витальевич
Подписано цифровой подписью: Троицкий Александр Витальевич

«УТВЕРЖДАЮ»
И.о. проректора
_____ А.В. Троицкий
«___»_____2023 г.

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.ДВ.04.02 «СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

Направление подготовки: 10.04.01 - Информационная безопасность
Направленность (профиль): Менеджмент информационной безопасности
Уровень высшего образования: Магистратура
Форма обучения: очная

Королев
2023

Рабочая программа является составной частью основной профессиональной образовательной программы и проходит рецензирование со стороны работодателей в составе основной профессиональной образовательной программы. Рабочая программа актуализируется и корректируется ежегодно.

Автор: Соляной В.Н. Рабочая программа дисциплины (модуля): Социальная инженерия в информационной безопасности. – Королев МО: «Технологический Университет», 2023

Рецензент: к.в.н., доцент Сухотерин А.И.

Рабочая программа составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по направлению подготовки магистров 10.04.01 Информационная безопасность и Учебного плана, утвержденного Ученым советом Университета. Протокол № 9 от 11.04.2023 года.

Рабочая программа рассмотрена и одобрена на заседании кафедры:

Заведующий кафедрой (ФИО, ученая степень, звание, подпись)	Соляной В.Н., к.в.н., доцент			
Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания кафедры	№8 от 29.03.2023г.			

Рабочая программа согласована:
Руководитель ОПОП ВО Сухотерин А.И.

Рабочая программа рекомендована на заседании УМС:

Год утверждения (переутверждения)	2023	2024		
Номер и дата протокола заседания УМС	№5 от 11.04.2023г.			

2

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП

Целью изучения дисциплины является углубленное изучение теоретических и прикладных основ социальной инженерии как научной дисциплины, связанной с созданием средств и методов выработки научно обоснованных управленческих решений в области информационной безопасности

В процессе обучения по направлению подготовки 10.04.01 «Информационная безопасность», студент приобретает и совершенствует следующие компетенции:

Универсальные компетенции:

- УК-5: Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия

Профессиональные компетенции:

- ПК-3: Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.
- ПК-4: Способен проводить занятия по избранным дисциплинам предметной области и разрабатывать методические материалы, используемые в образовательной деятельности направления менеджмент ИБ.

Основными задачами дисциплины являются:

1. раскрытие сущности, целей социальной инженерии (СИ) как метода несанкционированного доступа к информации или системам хранения информации без использования технических средств;
2. определение общих методологических подходов построения систем защиты информации с учетом возможных атак с использованием технологии социальной инженерии;
3. освоение методических подходов, установления состава защищаемой информации и выявления объектов защиты, подверженных атакам со стороны социального хакерства;
4. выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников, использующих методы социальной инженерии);
5. овладение методами оценки уязвимости защищаемой информации;
6. определение методов выявления параметров и структуры систем защиты информации;
7. освоение методов установления целесообразного состава мероприятий по защите информации от социального хакерства;
8. определение методологических подходов оценки эффективности

мер по защите информации от воздействия со стороны атак с использованием методов социальной инженерии.

Показатель освоения компетенции отражают следующие индикаторы:

Трудовые действия:

-УК-5.3. Применяет методы и навыки эффективного межкультурного взаимодействия, обеспечивает создание дружественной, деловой среды взаимодействия при выполнении профессиональных задач

- ПК-4.3. Проводить учебные занятия, контроль и оценка их освоения обучающихся учебных курсов, дисциплин, программ бакалавриата и ДПП (дополнительной профессиональной подготовки).

- ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.

Необходимые умения:

- УК-5.2. Анализирует и учитывает разнообразие культур в процессе межкультурного взаимодействия, выстраивает профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп

- ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.

- ПК-4.2. Выполнять технологии, осваиваемые обучающимися и реализовывать задания предусмотренные программой учебного курса (дисциплины).

Необходимые знания:

- УК-5.1. Использует технологии эффективного межкультурного взаимодействия, анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития, обосновывает актуальность их использования при профессиональном взаимодействии

- ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.

- ПК-4.1. Знать особенности организации образовательного процесса, методики разработки применения фонда оценочных средств и требования охраны труда при проведении всех видов учебных занятий.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП ВО

Дисциплина относится к дисциплинам по выбору части, формируемой участниками образовательных отношений, основной профессиональной образовательной программы подготовки магистров по направлению подготовки 10.04.01 «Информационная безопасность».

Дисциплина реализуется кафедрой информационной безопасности.

Дисциплина базируется на ранее изученных дисциплинах: «Современная философия и методология науки»; «Основы теории информационной безопасности», «Защищенные информационные системы» и компетенциях: УК-1, 2; ПК-1, 3; ОПК-1.

Знания и компетенции, полученные при изучении дисциплины необходимы при освоении одновременно изучаемых дисциплин “Организационно-правовые механизмы обеспечения информационной безопасности, “Экономико-управленческие аспекты обеспечения информационной безопасности” и для написания магистерской диссертации.

Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 часа

Виды занятий	Всего часов	Семестр 2	Семестр …	Семестр …	Семестр …
Общая трудоемкость	**72**	**72**			
ОЧНАЯ ФОРМА ОБУЧЕНИЯ					
Аудиторные занятия	**38**	**38**			
Лекции (Л)	**16**	**16**			
Практические занятия (ПЗ)	**16**	**16**			
Лабораторные работы (ЛР)					
Другие виды контактной работы*	**6**	**6**			
Практическая подготовка	**нет**	**нет**			
Самостоятельная работа	**34**	**34**			
Курсовые, расчетно-графические работы					
Контроль самостоятельной работы студентов	+	+			
Контрольная работа, домашнее задание	+	+			
Текущий контроль знаний (7 - 8, 15 - 16 недели)					
Вид итогового контроля	**Зачет**	**Зачет**			

* Под другими видами контактной работы понимается: групповые и индивидуальные консультации, тестирование.

1. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

1.1.Темы дисциплины и виды занятий

Таблица 2

Наименование тем	Лекции, час.	Практические занятия час.	Занятия в интерактивной форме, час.	Код компетенций
Раздел (модуль) 1. Теоретические основы информационной безопасности в условиях использования технологии социальной инженерии				
Тема 1. Введение. Социальная инженерия как технология несанкционированного доступа к информации или системам хранения информации без использования технических средств	2	2	0.5	УК-5 ПК-3 ПК-4
Тема 2. Техники и термины социальной инженерии, используемые для несанкционированного доступа к конфиденциальной информации	2	2	0.5	ПК-3 ПК-4
Тема 3. Теоретико-методологические основы оценки уязвимости информационных объектов с учетом возможных воздействий с использованием технологии социальной инженерии	2	2	1	УК-5 ПК-4
Тема 4. Методологические основы определения требований к информационной безопасности с учетом возможностей и развития технологии социальной инженерии	2	2	1	УК-5
Раздел (модуль) 2. Прикладные основы защиты информации от атак со стороны социального хакерства (социальной инженерии)				

Тема 5. Методология формирования комплексных систем информационной безопасности против атак со стороны социального хакерства. Защита пользователей	3	4	1	УК-5 ПК-3
Тема 6. Особенности управления информационной безопасностью в условиях воздействия со стороны социальной инженерии	3	2	1	УК-5 ПК-4
Тема 7. Перспективы развития теории и практики информационной безопасности с учетом противодействия несанкционированному доступу к информации с использованием технологии социальной инженерии	2	2	1	ПК-3 ПК-4
Итого:	**16**	**16**	**6**	

1.2.Содержание тем дисциплины

Тема 1. Введение. Социальная инженерия как технология несанкционированного доступа к информации или системам хранения информации без использования технических средств

Предмет и задачи курса. Значение и место курса в подготовке магистров по информационной безопасности. Взаимосвязь курса с другими дисциплинами. Разделы и темы, их распределение по видам аудиторных занятий. Формы проведения контрольных мероприятий. Формы проверки знаний. Состав и методика самостоятельной работы студентов по изучению дисциплины. Знания и умения студентов, которые должны быть получены в результате изучения курса. Рекомендованная научная и учебная литература. Характеристика существующих проблем по информационной безопасности в ходе становления современного информационного общества и развития технологии социальной инженерии. Социальная инженерия как составная часть социологии, использующая тех специфических знаний, которые направляют, приводят в порядок и оптимизируют процесс создания, модернизации и воспроизведение новых («искусственных») социальных реальностей. Анализ исторического развития подходов к обеспечению информационной

безопасности в мире и в Российской Федерации. Современная постановка задачи по обеспечению информационной безопасности. Переход к интенсивным мерам по обеспечению информационной безопасности в условиях развития технологии социальной инженерии.

Тема 2. Техники и термины социальной инженерии, используемые для несанкционированного доступа к конфиденциальной информации

Особенности принятия людьми решений, называемых когнитивным базисом, как основа техники социальной инженерии. Использование особенностей принятия решения, основанных на человеческой и социальной психологии, т.е. на том, что человек должен кому-либо доверять в социальной среде воспитания как методология социальной инженерии.

Претекстинг — действие, отработанное по заранее составленному сценарию (претексту).
Фишинг — техника, направленная на жульническое получение конфиденциальной информации.
Троянский конь — техника, эксплуатирующая любопытство, либо алчность цели. **Дорожное яблоко** — метод атаки, представляющий собой адаптацию троянского коня и использующий физические носители.
Кви про кво — технология, позволяющая злоумышленнику запустить вредоносное программное обеспечение.

Тема 3. Теоретико-методологические основы оценки уязвимости информационных объектов с учетом возможных воздействий с использованием технологии социальной инженерии

Понятие и системная классификация современных информационных угроз, включая социальную инженерию. Методология аналитико-синтетического мышления и знания формализованных процедур (технологий) конструкторско-изобретательской деятельности. Основные теоретико-прикладные показатели уязвимости защищаемого информационного ресурса. Методологические основы достоверности прогнозирования уязвимости информационных объектов. Теоретико-прикладные модели оценки ущерба от реализации информационных угроз со стороны социальной инженерии. Обратная социальная инженерия. Цель обратной социальной инженерии (reverse social engineering). Техники обратной социальной инженерии:

1. Диверсия;
2. Реклама.

Тема 4. Методологические основы определения требований к информационной безопасности с учетом возможностей и развития технологии социальной инженерии

Параметры безопасности информации и эффективности ее защиты от проникновения со стороны социальной инженерии. Методология оценки основных факторов, влияющих на требуемый уровень обеспечения информационной безопасности.

Тема 5. Методология формирования комплексных систем информационной безопасности против атак со стороны социального хакерства

Защита пользователей от социальной инженерии.
Системный подход как основа построения современных комплексов обеспечения информационной безопасности в условиях воздействия со стороны социальной инженерии. Определение, типизация и стандартизация систем обеспечения информационной безопасности. Комплексные системы информационной безопасности как многокритериальные развивающие объекты, отвечающие на вызовы социальной инженерии. Современные методологии проектирования комплексных систем обеспечения информационной безопасности, учитывающие нарастающее воздействие со стороны социальной инженерии. Методологические основы оценки эффективности функционирования комплексных систем информационной безопасности в условиях нарастающего воздействия со стороны социального хакерства.

Тема 6. Особенности управления информационной безопасностью в условиях воздействия со стороны социальной инженерии

Общая задача по управлению информационной безопасностью. Типовая модель управления информационной безопасностью с подсистемой защиты от социального хакерства. Общие положения и концепции управления информационной безопасностью. Виды управления информационной безопасностью: краткосрочное; среднесрочное и долгосрочное. Разработка системы администрирования, содержащей регламент и требования в отношении защиты от социальной инженерии.

Методологические основы выработки управленческих решений по информационной безопасности и характеристика основных этапов принятия и реализации решений. Основы оптимизации управленческих решений по информационной безопасности.

Основы организации обеспечения информационной безопасности государства и региона. Функции, задачи, структура и организация работы

региональных центров информационной безопасности с учетом возможных атак со стороны социальной инженерии.

Тема 7. Перспективы развития теории и практики информационной безопасности с учетом противодействия несанкционированному доступу к информации с использованием технологии социальной инженерии

Анализ состояния и прогноз развития теории информационной безопасности с учетом возрастающего негативного воздействия со стороны социальной инженерии. Разработка модели специализированных центров информационной безопасности, оснащенных средствами защиты от социальной инженерии. Перспективы развития межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности с программой и курсами, содержащими рекомендации по защите от социального хакерства.

2. Перечень учебно-методического обеспечения для самостоятельной работы по дисциплине (модулю)

«Методические указания для самостоятельной работы обучающихся по освоению дисциплины» представлены в Приложении 2.

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

Структура фонда оценочных средств, для проведения промежуточной аттестации обучающихся по дисциплине приведена в Приложении 1.

4. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1.Малинин, В. Н. Статистические методы анализа гидрометеорологической информации : учебник : в 2 томах / В. Н. Малинин. — 2 изд., испр. и доп. — Санкт-Петербург : РГГМУ, 2020 — Том 1 : Первичный анализ и построение эмпирических зависимостей — 2020. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254123 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Малинин, В. Н. Статистические методы анализа гидрометеорологической информации : учебник : в 2 томах / В. Н. Малинин. — 2 изд., испр. и доп. — Санкт-Петербург : РГГМУ, 2020 — Том 2 : Анализ временных рядов и случайных полей — 2020. — 196 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254126 (дата обращения: 28.11.2022). — Режим доступа: для авториз. Пользователей

Дополнительная литература:

3.Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. 3.Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5178 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

8.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1. http://www.biblioclub.ru
2. http://znanium.com

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Методические указания для обучающихся по освоению дисциплины (модуля) приведены в Приложении 2 к настоящей рабочей программе.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**
  1. Электронные ресурсы образовательной среды Университета.
  2. Информационно-справочные системы (Консультант+; Гарант)

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия:

- аудитория, оснащенная презентационной техникой (проектор, экран);
- комплект электронных презентаций / слайдов.

Практические занятия:

- Аудитория, оснащенная мультимедийными средствами (проектор, ноутбук), демонстрационными материалами (наглядными пособиями).
- рабочее место преподавателя, оснащенное ПК с доступом в глобальную сеть Интернет ;
- рабочие места студентов, оснащенные компьютерами с доступом в глобальную сеть Интернет.

Самостоятельная работа студентов может проводится как в специально оборудованных компьютерных классах университета с выходом в Интернет, так и в домашних условиях при наличии Интернет – сети

Задание

ЗАДАНИЕ №1

Тема: Теоретические аспекты и практическое применение Федерального закона «О безопасности» №390-ФЗ от 28.12.2010

Цель работы.

Изучение основных принципов обеспечения защиты настоящего Федерального закона, его правовой основы, международного сотрудничества, а также полномочий федеральных органов исполнительной власти и статуса Совета Безопасности.

Продолжительность занятия: полтора учебных часа.

Задания.

1. Изучить теоретическую часть Лабораторной работы №1.
2. Выполнить практическую часть Лабораторной работы №1:
   а) ответить на вопросы для самопроверки;
   б) выполнить практические задания.
3. Предоставить отчет о выполненной работе преподавателю в виде документа Word.

Теоретическая часть.

Настоящий Федеральный закон определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством Российской Федерации (далее - безопасность, национальная безопасность), полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного

самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации (далее - Совет Безопасности).

Основными принципами обеспечения безопасности являются:

1) соблюдение и защита прав и свобод человека и гражданина;

2) законность;

3) системность и комплексность применения федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, другими государственными органами, органами местного самоуправления политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности;

4) приоритет предупредительных мер в целях обеспечения безопасности;

5) взаимодействие федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, других государственных органов с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности.

Правовую основу обеспечения безопасности составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, настоящий Федеральный закон, другие федеральные законы и иные нормативные правовые акты Российской Федерации, законы и иные нормативные правовые акты субъектов Российской Федерации, органов местного самоуправления, принятые в пределах их компетенции в области безопасности.

Координацию деятельности по обеспечению безопасности осуществляют Президент Российской Федерации и формируемый, и возглавляемый им Совет Безопасности, а также в пределах своей компетенции Правительство Российской Федерации, федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации, органы местного самоуправления.

1. Международное сотрудничество Российской Федерации в области обеспечения безопасности осуществляется на основе общепризнанных принципов и норм международного права и международных договоров Российской Федерации.

2. Основными целями международного сотрудничества в области обеспечения безопасности являются:

1) охрана суверенитета Российской Федерации, ее независимости и государственной целостности, предотвращение внутренних и внешних угроз, пресечение действий, направленных на отчуждение части территории Российской Федерации, а также призывов к таким действиям;

(Пункт в редакции, введенной в действие с 20 ноября 2020 года Федеральным законом от 9 ноября 2020 года N 365-ФЗ);

2) защита прав и законных интересов российских граждан за рубежом;

3) укрепление отношений со стратегическими партнерами Российской Федерации;

4) участие в деятельности международных организаций, занимающихся проблемами обеспечения безопасности;

5) развитие двусторонних и многосторонних отношений в целях выполнения задач обеспечения безопасности;

6) содействие урегулированию конфликтов, включая участие в миротворческой деятельности.

3. Решения межгосударственных органов, принятые на основании положений международных договоров Российской Федерации в их истолковании, противоречащем Конституции Российской Федерации, не подлежат исполнению в Российской Федерации.

(Часть дополнительно включена с 20 ноября 2020 года Федеральным законом от 9 ноября 2020 года N 365-ФЗ).

Полномочия Президента Российской Федерации в области обеспечения безопасности

Президент Российской Федерации:

1) определяет основные направления государственной политики в области обеспечения безопасности;

2) утверждает стратегию национальной безопасности Российской Федерации, иные концептуальные и доктринальные документы в области обеспечения безопасности;

3) формирует и возглавляет Совет Безопасности;

4) устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых он осуществляет;

5) в порядке, установленном Федеральным конституционным законом от 30 мая 2001 года N 3-ФКЗ "О чрезвычайном положении", вводит на территории Российской Федерации или в отдельных ее местностях чрезвычайное положение, осуществляет полномочия в области обеспечения режима чрезвычайного положения;

6) принимает в соответствии с законодательством Российской Федерации:

а) решение о применении специальных экономических мер в целях обеспечения безопасности;

б) меры по защите граждан от преступных и иных противоправных действий, по противодействию терроризму и экстремизму;

7) решает в соответствии с законодательством Российской Федерации вопросы, связанные с обеспечением защиты:

а) информации и государственной тайны;

б) населения и территорий от чрезвычайных ситуаций;

8) осуществляет иные полномочия в области обеспечения безопасности, возложенные на него Конституцией Российской Федерации, федеральными конституционными законами и федеральными законами.

Полномочия палат Федерального Собрания Российской Федерации в области обеспечения безопасности

1. Совет Федерации Федерального Собрания Российской Федерации:

1) рассматривает принятые Государственной Думой Федерального Собрания Российской Федерации федеральные законы в области обеспечения безопасности;

2) утверждает указ Президента Российской Федерации о введении чрезвычайного положения;

3) проводит консультации по предложенным Президентом Российской Федерации кандидатурам на должность руководителей федеральных органов исполнительной власти (включая федеральных министров), ведающих вопросами обороны, безопасности государства, внутренних дел, юстиции, иностранных дел, предотвращения чрезвычайных ситуаций и ликвидации последствий стихийных бедствий, общественной безопасности.

(Пункт дополнительно включен с 20 ноября 2020 года Федеральным законом от 9 ноября 2020 года N 365-ФЗ)

2. Государственная Дума Федерального Собрания Российской Федерации принимает федеральные законы в области обеспечения безопасности.

Полномочия Правительства Российской Федерации в области обеспечения безопасности

Правительство Российской Федерации:

1) участвует в определении основных направлений государственной политики в области обеспечения безопасности;

2) формирует федеральные целевые программы в области обеспечения безопасности и обеспечивает их реализацию;

3) устанавливает компетенцию федеральных органов исполнительной власти в области обеспечения безопасности, руководство деятельностью которых оно осуществляет;

4) организует обеспечение федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, органов местного самоуправления средствами и ресурсами, необходимыми для выполнения задач в области обеспечения безопасности;

5) осуществляет иные полномочия в области обеспечения безопасности, возложенные на него Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами и нормативными правовыми актами Президента Российской Федерации.

Полномочия федеральных органов исполнительной власти в области обеспечения безопасности

Федеральные органы исполнительной власти выполняют задачи в области обеспечения безопасности в соответствии с Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, нормативными правовыми актами Президента Российской Федерации и нормативными правовыми актами Правительства Российской Федерации.

Статус Совета Безопасности

1. Совет Безопасности является конституционным совещательным органом, осуществляющим содействие главе государства в реализации его полномочий по вопросам обеспечения национальных интересов и безопасности личности, общества и государства, а также поддержания гражданского мира и согласия в стране, охраны суверенитета Российской Федерации, ее независимости и государственной целостности, предотвращения внутренних и внешних угроз.

(Часть в редакции, введенной в действие с 20 ноября 2020 года Федеральным законом от 9 ноября 2020 года N 365-ФЗ).

2. Совет Безопасности формируется и возглавляется Президентом Российской Федерации.

3. Положение о Совете Безопасности Российской Федерации утверждается Президентом Российской Федерации.

4. В целях реализации задач и функций Совета Безопасности Президентом Российской Федерации могут создаваться рабочие органы Совета Безопасности и аппарат Совета Безопасности.

Практическая часть

а) Контрольные вопросы.

1) В каком году был издан ФЗ «О безопасности»?

2) Назовите основные цели в области обеспечения безопасности настоящего федерального закона.

3) Какие полномочия в области обеспечения безопасности у Правительства РФ в соответствии с №390-ФЗ?

4) Какие документы составляют правовую основу в области обеспечения безопасности?

5) Кто осуществляет координацию деятельности в области обеспечения безопасности?

б) Практические задания.

1. Возможно ли привести Федеральный закон «О безопасности» №390-ФЗ к антитеррористическим мероприятиям в типовом предприятии? Если возможно, описать:

1) работу с персоналом;

2) рекомендации в случае с террористическими действиями;

3) рекомендации в случае обнаружения подозрительного предмета;

4) памятку генеральным директорам, руководителям подразделений, а также обычным сотрудникам в случае обнаружения или в случае предупреждения террористического акта.

2. Выберите объект (организацию, учреждение и т.п.) и приведите собственную рекомендацию правил по безопасности, направленную на один вид деструктивного воздействия на персонал и/или объект.

Пример практического задания

Памятка по безопасности в сети Интернет

С каждым годом молодежи в интернете становиться больше, а школьники одни из самых активных пользователей Рунета. Между тем, помимо огромного количества возможностей, интернет несет и проблемы. Эта памятка должна помочь тебе безопасно находиться в сети.

Компьютерный вирус – это разновидность компьютерных программ, отличительной особенностью которой является способность к размножению. В дополнение к этому, вирусы могут повредить или полностью уничтожить все файлы и данные, подконтрольные пользователю, от имени которого была запущена заражённая программа, а также повредить или даже уничтожить операционную систему со всеми файлами в целом. В большинстве случаев распространяются вирусы через интернет.

Методы защиты от вредоносных программ:

- Используй современные операционные системы, имеющие серьёзный уровень защиты от вредоносных программ;
- Постоянно устанавливай патчи (цифровые заплатки, которые автоматически устанавливаются с целью доработки программы) и другие обновления своей операционной системы. Скачивай их только с официального сайта разработчика ОС. Если существует режим автоматического обновления, включи его;
- Работай на своем компьютере под правами пользователя, а не администратора. Это не позволит большинству вредоносных программ инсталлироваться на твоем персональном компьютере;
- Используй антивирусные программные продукты известных производителей, с автоматическим обновлением баз;
- Ограничь физический доступ к компьютеру для посторонних лиц;
- Используй внешние носители информации, такие как флешка, диск или файл из интернета, только из проверенных источников;

- Не открывай компьютерные файлы, полученные из ненадёжных источников. Даже те файлы, которые прислал твой знакомый. Лучше уточни у него, отправлял ли он тебе их.

Советы по безопасной работе в общедоступных сетях Wi-Fi

Wi-Fi - это не вид передачи данных, не технология, а всего лишь бренд, марка. Еще в 1991 году нидерландская компания зарегистрировала бренд «WECA», что обозначало словосочетание «WirelessFidelity», который переводится как «беспроводная точность». До нашего времени дошла другая аббревиатура, которая является такой же технологией. Это аббревиатура «Wi-Fi». Такое название было дано с намеком на стандарт высший звуковой техники Hi-Fi, что в переводе означает «высокая точность».

Советы по безопасности работе в общедоступных сетях Wi-fi:

- Не передавай свою личную информацию через общедоступные Wi-Fi сети. Работая в них, желательно не вводить пароли доступа, логины и какие-то номера;
- Используй и обновляй антивирусные программы и брандмауер. Тем самым ты обезопасишь себя от закачки вируса на твое устройство;
- При использовании Wi-Fi отключи функцию «Общий доступ к файлам и принтерам». Данная функция закрыта по умолчанию, однако некоторые пользователи активируют её для удобства использования в работе или учебе;
- Не используй публичный WI-FI для передачи личных данных, например для выхода в социальные сети или в электронную почту;
- Ипользуй только защищенное соединение через HTTPS, а не HTTP, т.е. при наборе веб-адреса вводи именно «https://»;
- В мобильном телефоне отключи функцию «Подключение к Wi-Fi автоматически». Не допускай автоматического подключения устройства к сетям Wi-Fi без твоего согласия.

Основные советы о безопасности в социальных сетях

Социальные сети активно входят в нашу жизнь, многие люди работают и живут там постоянно, а в Facebook уже зарегистрирован миллиард человек, что

является одной седьмой всех жителей планеты. Многие пользователи не понимают, что информация, размещенная ими в социальных сетях, может быть найдена и использована кем угодно, в том числе не обязательно с благими намерениями.

Основные советы по безопасности в социальных сетях:

- Ограничь список друзей. У тебя в друзьях не должно быть случайных и незнакомых людей;
- Защищай свою частную жизнь. Не указывай пароли, телефоны, адреса, дату твоего рождения и другую личную информацию. Злоумышленники могут использовать даже информацию о том, как ты и твои родители планируете провести каникулы;
- Защищай свою репутацию - держи ее в чистоте и задавай себе вопрос: хотел бы ты, чтобы другие пользователи видели, что ты загружаешь? Подумай, прежде чем что-то опубликовать, написать и загрузить;
- Если ты говоришь с людьми, которых не знаешь, не используй свое реальное имя и другую личную информации: имя, место жительства, место учебы и прочее;
- Избегай размещения фотографий в Интернете, где ты изображен на местности, по которой можно определить твое местоположение;
- При регистрации в социальной сети необходимо использовать сложные пароли, состоящие из букв и цифр и с количеством знаков не менее 8;
- Для социальной сети, почты и других сайтов необходимо использовать разные пароли. Тогда если тебя взломают, то злоумышленники получат доступ только к одному месту, а не во все сразу.

Основные советы по безопасной работе с электронными деньгами

Электронные деньги — это очень удобный способ платежей, однако существуют мошенники, которые хотят получить эти деньги.

Электронные деньги появились совсем недавно и именно из-за этого во многих государствах до сих пор не прописано про них в законах. В России же они

функционируют и о них уже прописано в законе, где их разделяют на несколько видов – анонимные и не анонимные. Разница в том, что анонимные - это те, в которых разрешается проводить операции без идентификации пользователя, а в неанонимных идентификации пользователя является обязательной. Также следует различать электронные фиатные деньги (равны государственным валютам) и электронные нефиатные деньги (не равны государственным валютам).

Основные советы по безопасной работе с электронными деньгами:

- Привяжи к счету мобильный телефон. Это самый удобный и быстрый способ восстановить доступ к счету. Привязанный телефон поможет, если забудешь свой платежный пароль или зайдешь на сайт с незнакомого устройства;
- Используй одноразовые пароли. После перехода на усиленную авторизацию тебе уже не будет угрожать опасность кражи или перехвата платежного пароля;
- Выбери сложный пароль. Преступникам будет не просто угадать сложный пароль. Надежные пароли — это пароли, которые содержат не менее 8 знаков и включают в себя строчные и прописные буквы, цифры и несколько символов, такие как знак доллара, фунта, восклицательный знак и т.п. Например, $tR0ng!;;
- Не вводи свои личные данные на сайтах, которым не доверяешь.

Основные советы по безопасной работе с электронной почтой

Электронная почта — это технология и предоставляемые ею услуги по пересылке и получению электронных сообщений, которые распределяются в компьютерной сети. Обычно электронный почтовый ящик выглядит следующим образом: имя_пользователя@имя_домена. Также кроме передачи простого текста, имеется возможность передавать файлы.

Основные советы по безопасной работе с электронной почтой:

- Надо выбрать правильный почтовый сервис. В интернете есть огромный выбор бесплатных почтовых сервисов, однако лучше доверять тем, кого знаешь и кто первый в рейтинге;

- Не указывай в личной почте личную информацию. Например, лучше выбрать «музыкальный_фанат@» или «рок2013» вместо «тема13»;
- Используй двухэтапную авторизацию. Это когда помимо пароля нужно вводить код, присылаемый по SMS;
- Выбери сложный пароль. Для каждого почтового ящика должен быть свой надежный, устойчивый к взлому пароль;
- Если есть возможность написать самому свой личный вопрос, используй эту возможность;
- Используй несколько почтовых ящиков. Первый для частной переписки с адресатами, которым ты доверяешь. Это электронный адрес не надо использовать при регистрации на форумах и сайтах;
- Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы;
- После окончания работы на почтовом сервисе перед закрытием вкладки с сайтом не забудь нажать на «Выйти».

Основные советы по борьбе с кибербуллингом

Кибербуллинг — преследование сообщениями, содержащими оскорбления, агрессию, запугивание; хулиганство; социальное бойкотирование с помощью различных интернет-сервисов.

Основные советы по борьбе с кибербуллингом:

- Не бросайся в бой. Лучший способ: посоветоваться как себя вести и, если нет того, к кому можно обратиться, то вначале успокоиться. Если ты начнешь отвечать оскорблениями на оскорбления, то только еще больше разожжешь конфликт;
- Управляй своей киберрепутацией;
- Анонимность в сети мнимая. Существуют способы выяснить, кто стоит за анонимным аккаунтом;
- Не стоит вести хулиганский образ виртуальной жизни. Интернет фиксирует все твои действия и сохраняет их. Удалить их будет крайне затруднительно;

- Соблюдай свой виртуальную честь смолоду;
- Игнорируй единичный негатив. Одноразовые оскорбительные сообщения лучше игнорировать. Обычно агрессия прекращается на начальной стадии;
- Бан агрессора. В программах обмена мгновенными сообщениями, в социальных сетях есть возможность блокировки отправки сообщений с определенных адресов;
- Если ты свидетель кибербуллинга. Твои действия: выступить против преследователя, показать ему, что его действия оцениваются негативно, поддержать жертву, которой нужна психологическая помощь, сообщить взрослым о факте агрессивного поведения в сети.

Основные советы по безопасности мобильного телефона

Современные смартфоны и планшеты содержат в себе вполне взрослый функционал, и теперь они могут конкурировать со стационарными компьютерами. Однако, средств защиты для подобных устройств пока очень мало. Тестирование и поиск уязвимостей в них происходит не так интенсивно, как для ПК, то же самое касается и мобильных приложений. Современные мобильные браузеры уже практически догнали настольные аналоги, однако расширение функционала влечет за собой большую сложность и меньшую защищенность. Далеко не все производители выпускают обновления, закрывающие критические уязвимости для своих устройств.

Основные советы для безопасности мобильного телефона:

- Ничего не является по-настоящему бесплатным. Будь осторожен, ведь когда тебе предлагают бесплатный контент, в нем могут быть скрыты какие-то платные услуги;
- Думай, прежде чем отправить SMS, фото или видео. Ты точно знаешь, где они будут в конечном итоге?
- Необходимо обновлять операционную систему твоего смартфона;
- Используй антивирусные программы для мобильных телефонов;

- Не загружай приложения от неизвестного источника, ведь они могут содержать вредоносное программное обеспечение;
- После того как ты выйдешь с сайта, где вводил личную информацию, зайди в настройки браузера и удали cookies;
- Периодически проверяй какие платные услуги активированы на твоем номере;
- Давай свой номер мобильного телефона только людям, которых ты знаешь и кому доверяешь;
- Bluetooth должен быть выключен, когда ты им не пользуешься. Не забывай иногда проверять это.

Основные советы по безопасности игрового аккаунта

Современные онлайн-игры – это красочные, захватывающие развлечения, объединяющие сотни тысяч человек по всему миру. Игроки исследуют данный им мир, общаются друг с другом, выполняют задания, сражаются с монстрами и получают опыт. За удовольствие они платят: покупают диск, оплачивают абонемент или приобретают какие-то опции.
Все эти средства идут на поддержание и развитие игры, а также на саму безопасность: совершенствуются системы авторизации, выпускаются новые патчи (цифровые заплатки для программ), закрываются уязвимости серверов. В подобных играх стоит опасаться не столько своих соперников, сколько кражи твоего пароля, на котором основана система авторизации большинства игр.

Основные советы по безопасности твоего игрового аккаунта:

- Если другой игрок ведет себя плохо или создает тебе неприятности, заблокируй его в списке игроков;
- Пожалуйся администраторам игры на плохое поведение этого игрока, желательно приложить какие-то доказательства в виде скринов;
- Не указывай личную информацию в профайле игры;
- Уважай других участников по игре;
- Не устанавливай неофициальные патчи и моды;

- Используй сложные и разные пароли;
- Даже во время игры не стоит отключать антивирус. Пока ты играешь, твой компьютер могут заразить.

Основные советы по борьбе с фишингом

Обычной кражей денег и документов сегодня уже никого не удивиfшь, но с развитием интернет-технологий злоумышленники переместились в интернет, и продолжают заниматься «любимым» делом. Так появилась новая угроза: интернет-мошенничества или фишинг, главная цель которого состоит в получении конфиденциальных данных пользователей — логинов и паролей. На английском языке phishing читается как фишинг (от fishing — рыбная ловля, password — пароль).

Основные советы по борьбе с фишингом:

- Следи за своим аккаунтом. Если ты подозреваешь, что твоя анкета была взломана, то необходимо заблокировать ее и сообщить администраторам ресурса об этом как можно скорее;
- Используй безопасные веб-сайты, в том числе, интернет-магазинов и поисковых систем;
- Используй сложные и разные пароли. Таким образом, если тебя взломают, то злоумышленники получат доступ только к одному твоему профилю в сети, а не ко всем;
- Если тебя взломали, то необходимо предупредить всех своих знакомых, которые добавлены у тебя в друзьях, о том, что тебя взломали и, возможно, от твоего имени будет рассылаться спам и ссылки на фишинговые сайты;
- Установи надежный пароль (PIN) на мобильный телефон;
- Отключи сохранение пароля в браузере;
- Не открывай файлы и другие вложения в письмах даже если они пришли от твоих друзей. Лучше уточни у них, отправляли ли они тебе эти файлы.

Основные советы по защите цифровой репутации

Цифровая репутация - это негативная или позитивная информация в сети о тебе. Компрометирующая информация размещенная в интернете может серьезным образом отразиться на твоей реальной жизни. «Цифровая репутация» - это твой имидж, который формируется из информации о тебе в интернете. Твое место жительства, учебы, твое финансовое положение, особенности характера и рассказы о близких – все это накапливается в сети.
Многие подростки легкомысленно относятся к публикации личной информации в Интернете, не понимая возможных последствий. Ты даже не сможешь догадаться о том, что фотография, размещенная 5 лет назад, стала причиной отказа принять тебя на работу.
Комментарии, размещение твоих фотографий и другие действия могут не исчезнуть даже после того, как ты их удалишь. Ты не знаешь, кто сохранил эту информацию, попала ли она в поисковые системы и сохранилась ли она, а главное: что подумают о тебе окружающее люди, которые найдут и увидят это. Найти информацию много лет спустя сможет любой – как из добрых побуждений, так и с намерением причинить вред. Это может быть кто угодно.

Основные советы по защите цифровой репутации:

- Подумай, прежде чем что-то публиковать и передавать у себя в блоге или в социальной сети;
- В настройках профиля установи ограничения на просмотр твоего профиля и его содержимого, сделай его только «для друзей»;
- Не размещай и не указывай информацию, которая может кого-либо оскорблять или обижать.

ЗАДАНИЕ №2

Тема: «Указ президента РФ от 01.05.2022г. №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».

Цель занятия: Изучить Указ президента РФ №250. Понять его суть, разобрать основные требования по информационной безопасности, которые должны быть реализованы в организациях, попадающих под действие указа.

Продолжительность занятия: 4 часа.

Задание:

1. Изложить суть Указа. Выделить ключевые идеи.
2. Выяснить на кого распространяется Указ №250.
3. Структурировать основных органов по обеспечению защиты информации.
4. Сформировать основные требования Указа №250.
5. Сделать заключение.

1. Суть Указа №250. Ключевые идеи.

Первого мая Президент России подписал указ № 250, направленный на обеспечение информационной безопасности ряда ключевых компаний России. К таким компаниям относятся некоторые органы власти, предприятия с государственным участием, субъекты критической информационной инфраструктуры (КИИ), стратегические и системообразующие организации. Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» официально вступил в силу со дня его опубликования, т. е. выполнять его требования необходимо уже с 1 мая 2022 г. Указ нацелен на повышение уровня информационной безопасности критически важных организаций РФ.

Можно выделить следующие ключевые идеи Указа №250:

1. Руководитель организации должен отвечать за информационную безопасность и у него должны быть соответствующие сотрудники для этого.
2. Информационная безопасность должна быть практической и результативной, учитывающей потребности и задачи организации.
3. Не должны применяться средства защиты из недружественных стран.

4. Подрядные организации, оказывающие услуги по ИБ должны иметь лицензии на осуществление деятельности по технической защите конфиденциальной информации.
5. К деятельности по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты теперь можно привлекать только аккредитованные центры государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА).
6. Организациям необходимо обеспечить постоянный мониторинг рекомендаций по нейтрализации актуальных угроз ИБ, которые им направляют ФСБ России и ФСТЭК России, с незамедлительной реализацией предписанных организационных и технических мер.

2. Область распространения Указа №250.

Ряд мер по повышению уровня безопасности информационных ресурсов необходимо выполнить следующим органам (организациям):

- федеральный орган исполнительной власти;
- высший исполнительный орган государственной власти субъекта РФ;
- государственный фонд;
- государственная компания;
- предприятие, созданное на основании федерального закона;
- стратегическое предприятие;
- стратегическое акционерное общество;
- системообразующая организация экономики (на уровне РФ или субъекта РФ);
- субъект критической информационной инфраструктуры (независимо от наличия значимых объектов КИИ).

Всего в России более 500 тысяч организаций, попавших по действие Указа №250.

Существуют государственные внебюджетные фонды, к которым могут быть отнесены:

- Пенсионный фонд Российской Федерации (ПФР);
- Фонд социального страхования Российской Федерации (ФСС);
- Федеральный фонд обязательного медицинского страхования (ФФОМС);
- Территориальные фонды обязательного медицинского страхования (ТФОМС).

Под действие указа также попадают и иные фонды, созданные государством, такие как:

- Фонд развития промышленности;
- Российский фонд прямых инвестиций;
- Российский фонд технологического развития;
- Финансовые фонды поддержки отраслей;
- Инвестиционные фонды и т.п.

Единого списка системообразующих предприятий не существует – он постоянно расширяется. Например, в апреле перечень только системообразующих промышленных предприятий в РФ был расширен до 1100 организаций. Перечень стратегических предприятий и стратегических акционерных обществ утвержден Указом Президента РФ от 04.08.2004 №1009 «Об утверждении Перечня стратегических предприятий и стратегических акционерных обществ». В список госкомпаний и госкомпаний входят Сбербанк, ВТБ, Роснефть, Почта России, РЖД и др.

3. Органы управления по обеспечению информационной безопасности

Указ №250 требует установить определенную структуру ответственности за обеспечение информационной безопасности:

1. Руководитель организации:
    - Возлагает на заместителя полномочия по информационной безопасности.

- Создает подразделение по информационной безопасности.
- При необходимости принимает решение о привлечении внешних организаций – лицензиатов ФСТЭК или аккредитованных ФСБ организаций.
- Несет персональную ответственность.

2. Заместитель руководителя организации:
    - Курирует деятельность по обеспечению информационной безопасности.
    - Взаимодействует с НКЦКИ.
    - Отвечает за согласование стратегии организации в части ИБ.
    - Согласовывает политику ИТ, ЦТ и цифровизации.
    - Осуществляет регулярный контроль.
    - Информирует руководство об инцидентах.
    - Руководит подразделением по информационной безопасности.
    - Входит в коллегиальный орган.
3. Подразделение по информационной безопасности:
    - Планирование, организация, координация и контроль работ по ИБ.
    - Выявление угроз ИБ и уязвимостей.
    - Предотвращение утечек информации.
    - Обеспечение киберустойчивости организации.
    - Взаимодействие с НКЦКИ.

Ответственные за Информационную безопасность должны владеть следующими знаниями:

- основные процессы организации и специфику обеспечения их информационной безопасности;
- влияние ИТ на деятельность организации;
- современные информационные и телекоммуникационные технологии;
- нормативные правовые акты в области ИБ и ЗИ;
- обеспечение информационной безопасности.

Заместитель руководителя организации, ответственный за обеспечение ИБ, имеет высшее образование (не ниже уровня специалитета или магистратуры) в сфере ИБ или прошел профпереподготовку
по программе длительностью не менее 360 часов, согласованной с ФСТЭК России или ФСБ России в соответствии с Приказом
Министерства образования и науки от 19.10.2020 № 1316, а также должен проходить повышение квалификации не менее одного раза в пять лет.

4. Основные требования Указа №250 по обеспечению информационной безопасности

В Указе №250, а также в подзаконных актах содержатся следующие основные требования по обеспечению информационной безопасности в организациях, которые попали под действие данного указа:

- Должна быть разработана и утверждена политика организации в области информационной безопасности.
- Должны быть определены цели обеспечения информационной безопасности.
- Должен быть сформулированный перечень недопустимых событий и негативный последствий(ущерба) для организации.
- Необходимо проводить оценку возможности возникновения и реализации недопустимых событий путем моделирования целевых атак.
- Должны проводиться мероприятия по недопущению и отслеживанию недопустимых событий и негативных последствий (ущерба).
- Должен проводиться контроль эффективности(результативности) мероприятий по недопущению и отслеживанию недопустимых событий и негативных последствий(ущерба).
- Должны реализовываться организационные и технические меры в области Информационной безопасности, требования о реализации которых направляются ФСТЭК России и ФСБ России.

- Должны быть организованы работы по формированию навыков и повышению осведомленности работников организации в сфере Информационной безопасности.
- Должен быть организованный контроль за соблюдением нормативных правовых актов в области Информационной безопасности.
- Необходимо осуществлять контроль пользователей организации в части соблюдения ими конфиденциальности информации и правил работы со съемными носителями информации.
- Должны быть спланированы мероприятия по обеспечению Информационной безопасности в подведомственных организациях, филиалах, представительствах (при их наличии)
- Должен проводиться контроль состояния ИБ, включая оценку защищенности, в подведомственных организациях, филиалах, представительствах (при их наличии).
- Должны проводиться регулярные практические учения по противодействию компьютерным атакам(киберучения).
- Должен проводится регулярный анализ и оценка новых угроз, способов и методов проведения компьютерных атак.
- Должен быть выстроен непрерывный процесс выявления и устранения угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств.
- Должна быть проведена оценка практической возможности использования нарушителями недостатков(уязвимостей) средств защиты информации и программного обеспечения (на примере наиболее критически важных).
- Должен быть выстроенный непрерывный процесс обнаружения, предотвращения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

5. Заключение

Указ Президента России от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» кардинально меняет подход к обеспечению кибербезопасности в российских компаниях.

Организациям сейчас нужно провести работы по распределению ответственности за обеспечение ИБ на должностных лиц. В дальнейшем, при необходимости, понадобится привести распорядительные документы о должностных обязанностях ко введённым Правительством РФ нормам. Также необходимо осуществлять мониторинг нормотворческой деятельности Правительства РФ по части выполнения распоряжений Указа и, в случае включения организации в состав ключевых органов (организаций), оперативно провести работы, по оценке защищённости информационных ресурсов. Организациям рекомендовано начать инвентаризацию эксплуатируемого оборудования с выявлением иностранного аппаратного и программного обеспечения, средств защиты информации, с планированием перехода на преимущественное использование отечественных разработок. Также необходимо провести работы по анализу привлекаемых подрядных организаций в области ИБ на наличие у них необходимых лицензий, в дальнейшем — на наличие аккредитации у центров ГосСОПКА. Компаниям в текущей ситуации необходимо быть готовыми к оперативному взаимодействию с регулирующими органами (ФСБ России, ФСТЭК России) и выполнению их указаний.

Список использованных источников

1. Указ Президента РФ от 1 мая 2022 г. № 250 "О дополнительных мерах по обеспечению информационной безопасности Российской Федерации".
2. Типовое техническое задание на выполнение работ по оценке уровня защищенности информационной инфраструктуры от 3 июня 2022 г.
3. Разъяснения к Указу Президента о дополнительных мерах по обеспечению ИБ (№ 250 от 01.05.2022) .
   URL: https://www.anti-malware.ru/analytics/Technology_Analysis/President-Decree-250-Clarifications
4. Указ 250: кто и как теперь отвечает за кибербезопасность, вебинар.
   URL: https://www.ptsecurity.com/ru-ru/research/webinar/ukaz-250-kto-i-kak-teper-otvechaet-za-kiberbezopasnost
5. Каким должно быть обучение руководителя по ИБ в соответствии с 250-м указом, Алексей Лукацкий.
   URL: https://lukatsky.ru/training/kakim-dolzhno-byt-obuchenie-rukovoditelya-po-ib-v-sootvetstvii-s-250-m-ukazom.html
6. Немного разъяснений по 250-му Указу Президента, Алексей Лукацкий.
   URL: https://lukatsky.ru/legislation/nemnogo-razyasneniy-po-250-mu-ukazu-prezidenta.html

Приложение 1

Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль: Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

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

№ п/п	Индекс компе-тенции	Содержание компетенции *	Раздел дисциплины, обеспечивающий формирование компетенции	В результате изучения раздела дисциплины, обеспечивающего формирование компетенции, обучающийся приобретает:		
				Трудовые действия	Необходимые умения	Необходимые знания
1.	УК-5	Способен анализировать и учитывать разнообразие культур в процессе межкультурного взаимодействия	Тема:1,2,3,4,5,6	УК-5.3. Применяет методы и навыки эффективного межкультурного взаимодействия, обеспечивает создание дружественной, деловой среды взаимодействия при выполнении профессиональных задач	УК-5.2. Анализирует и учитывает разнообразие культур в процессе межкультурного взаимодействия, выстраивает профессиональное взаимодействие с учетом особенностей основных форм научного и религиозного сознания, деловой и общей культуры представителей других этносов и конфессий, различных социальных групп	УК-5.1. Использует технологии эффективного межкультурного взаимодействия, анализирует важнейшие идеологические и ценностные системы, сформировавшиеся в ходе исторического развития, обосновывает актуальность их использования при профессиональном взаимодействии

4.	ПК-3	Способен осуществлять анализ и систематизацию научно-технической информации, вырабатывать и внедрять научно-обоснованные решения в области защищенных технологий АИАД (автоматизированной информационно-аналитической деятельности.	Тема:1,2,3,4,5,6,7	ПК-3.3. Организует научно-исследовательскую деятельность на основе тенденций развития, области научного знания и рынка труда.	ПК-3.2. Определять актуальность тематики исследовательской деятельности, формулировать темы НИР и оказывать методическую помощь в их выполнении.	ПК-3.1. Знать проблемы и тенденции развития научной области и профессиональной деятельности, а также теоретические основы и технологии организации научно-исследовательской работы и требования к оформлению исследовательских разработок.
5.	ПК-4	Способен проводить занятия по избранным дисциплинам предметной области и разрабатывать методические материалы, используемые в образовательной деятельности направления менеджмент ИБ.	Тема:1,2,3,4,5,6	ПК-4.3. Проводить учебные занятия, контроль и оценка их освоения обучающихся учебных курсов, дисциплин, программ бакалавриата и ДПП (дополнительной профессиональной подготовки).	ПК-4.2. Выполнять технологии, осваиваемые обучающимися и реализовывать задания предусмотренные программой учебного курса (дисциплины).	ПК-4.1. Знать особенности организации образовательного процесса, методики разработки применения фонда оценочных средств и требования охраны труда при проведении всех видов учебных занятий.

2.Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	*Инструменты, оценивающие сформированность компетенции*	*Этапы и показатель оценивания компетенции*	*Критерии оценивания компетенции на различных этапах формирования и шкалы оценивания*
УК-5 ПК-3,4	***Тест***	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 90% правильных ответов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 70% правильных ответов;*** • ***компетенция освоена на <u>базовом</u> уровне – от 51% правильных ответов;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – менее 50% правильных ответов***	***Например:*** ***Проводится письменно. Время, отведенное на процедуру - 30 минут.*** ***Неявка – 0 баллов.*** ***Критерии оценки определяются процентным соотношением.*** ***Неудовлетворительно – менее 50% правильных ответов.*** ***Удовлетворительно - от 51% правильных ответов.*** ***Хорошо - от 70%.*** ***Отлично – от 90%.*** ***Максимальная оценка – 5 баллов.***
УК-5 К-3,4	Доклад	***А) полностью сформирована (компетенция освоена на <u>высоком</u> уровне) – 5 баллов*** ***Б) частично сформирована:*** • ***компетенция освоена на <u>продвинутом</u> уровне – 4 балла;*** • ***компетенция освоена на <u>базовом</u> уровне – 3 балла;*** ***В) не сформирована (<u>компетенция не сформирована</u>) – 2 и менее баллов***	Проводится устно с использованием мультимедийных систем, а также с использованием технических средств Время, отведенное на процедуру – 10 - 15 мин. Неявка – 0. Критерии оценки: 1.Соответствие представленной презентации заявленной тематике (1 балл). 2.Качество источников и их количество при подготовке доклада и разработке презентации (1 балл). 3.Владение информацией и способность отвечать на вопросы аудитории (1 балл). 4.Качество самой представленной презентации (1 балл). 5.Оригинальность подхода и всестороннее раскрытие выбранной тематики (1 балл). Максимальная сумма баллов - 5 баллов. Результаты оценочной процедуры представляются обучающимся непосредственно в день проведения презентации – для текущего контроля. Оценка проставляется в электронный журнал.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

3.1.Примерная тематика докладов в форме презентаций:

1. История и формирование понятия «социальная инженерия».
2. Социальная инженерия и социальные хакеры.
3. Социальная инженерия – основной инструмент современных хакеров.
4. Взломы защищенного информационного ресурса методами социальной инженерии.
5. Социальное программирование как метод социальной инженерии.
6. Построение социальных файрволов.
7. Психологические аспекты подготовки социальных хакеров.
8. Искусство ведения переговоров.
9. Типология психологической личности.
10. Область социальной инженерии – финансовые махинации.
11. Область социальной инженерии – маркетинговые планы организации.
12. Область социальной инженерии – воровство клиентских баз данных.
13. Область социальной инженерии – рейдерские атаки.
14. Правила убеждений – инструмент социального хакера.
15. Психологические особенности поведения человека в толпе.

3.2.Примерная тематика докладов форме презентаций (вариант 2)

1. Новые методы исследования информационной безопасности в области социальной инженерии.
2. Современные методы обеспечения информационной безопасности в социальной инженерии.
3. Анализ угроз информационной безопасности объектов в области социальной инженерии.
4. Особенности разработки методов противодействия социальным хакерам.
5. Отечественные и международные стандарты по защите информации в социальной сфере.
6. Разработка проектов методических документов в области социальной инженерии как особой области информационной безопасности.
7. Разработка проектов нормативных документов, технической документации в области социальной инженерии как особой области информационной безопасности.
8. Разработка проектов технической документации в области социальной инженерии как особой области информационной безопасности.

9. Предложения и мероприятия по реализации разработанных проектов и программ в области социальной инженерии как особой области информационной безопасности.
10. Социальная инженерия как метода несанкционированного доступа к информации или системам хранения информации ограниченного пользования.
11. Общие методологические подходы построения систем защиты информации с учетом возможных атак с использованием технологии социальной инженерии.
12. Методические подходы, установления состава защищаемой информации и выявления объектов защиты, подверженных атакам со стороны социального хакерства.
13. Методы определения актуальных информационных угроз и опасных нарушителей (злоумышленников), использующих методы социальной инженерии.
14. Методы установления целесообразного состава мероприятий по защите информации от социального хакерства.
15. Особенности методов управления информационной безопасностью объектов в условиях воздействия социальных хакеров.
16. Оценка эффективности мер по защите информации от воздействия со стороны атак с использованием методов социальной инженерии.
17. Виды уязвимости защищаемой информации и формы ее проявления с учетом возможных атак с использованием методов социальной инженерии
18. Источники, виды и способы дестабилизирующего воздействия на защищаемую информацию со стороны социальной сферы
19. Каналы и методы несанкционированного доступа к конфиденциальной информации социального хакерства.
20. Классификация видов, методов и средств, обеспечивающих защиту информации от социального хакерства.
21. Технологическое обеспечение защиты информации с учетом возможных атак с использованием методов социальной инженерии.
22. Кадровое обеспечение защиты информации с учетом возможных атак с использованием методов социальной инженерии.
23. Ресурсное обеспечение защиты информации с учетом возможных атак с использованием методов социальной инженерии.
24. Направления и виды защиты информации с учетом характера информации и задач по ее защите в области социальной инженерии;
25. Комплексный подход по защите информации в регионе с учетом возможных атак с использованием технологии социальной инженерии.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Формой контроля знаний по дисциплине «Социальная инженерия в информационной безопасности» являются две текущие аттестации в виде тестов и итоговая аттестация в виде зачета.

Неделя текущего контроля	Вид оценочного средства	Код компетенций, оценивающий знания, умения, навыки	Содержание оценочного средства	Требования к выполнению	Срок сдачи (неделя семестра)	Критерии оценки по содержанию и качеству с указанием баллов
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-5 ПК-3 ПК-4	20 вопросов	Компьютерное тестирование ; время отведенное на процедуру - 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установленные графиком образовательного процесса	тестирование	УК-5 ПК-3 ПК-4	20 вопросов	Компьютерное тестирование; время отведенное на процедуру – 30 минут	Результаты тестирования предоставляются в день проведения процедуры	***Преподаватель указывает критерии оценки данного вида контроля. Например, критерии оценки определяются процентным соотношением. Неявка – 0. Неудовлетворительно – менее 50% правильных ответов Удовлетворительно - от 51% правильных ответов. Хорошо - от 70%. Отлично – от 90%***
Проводится в сроки, установленные	Зачет	УК-5 ПК-3 ПК-4	3 вопроса	Зачет проводится в письменной форме, путем ответа на вопросы.	Результаты предоставляются в день проведения зачета	Критерии оценки: **«Зачтено»:** • знание основных понятий предмета;

графиком образовательного процесса				Время, отведенное на процедуру – 30 минут.		• умение использовать и применять полученные знания на практике; • работа на семинарских занятиях; • знание основных научных теорий, изучаемых предметов; • ответ на вопросы билета. **«Не зачтено»**: демонстрирует частичные знания по темам дисциплин; • незнание основных понятий предмета; • неумение использовать и применять полученные знания на практике; • не работал на семинарских занятиях; • не отвечает на вопросы.

Итоговое начисление баллов по дисциплине осуществляется в соответствии с разработанной и внедренной балльно-рейтинговой системой контроля и оценивания уровня знаний и внеучебной созидательной активности обучающихся.

Вопросы, выносимые на зачёт

1. Существующие проблемы по информационной безопасности в современном информационном обществе.
2. Определение и содержание метода социальной инженерии (СИ).
3. Исторический аспект возникновения и развития технологии социальной инженерии.
4. Социальная инженерия как оружие в современной системе для взлома защиты информационной.

5. Социальная инженерия как составная часть социологии, претендующая на совокупность специфических знаний, направляющих, приводящих в порядок и оптимизирующих процесс создания, модернизации и воспроизведение новых («искусственных») социальных реальностей.
6. Базовое содержание основ теории информационной безопасности.
7. Понятие и системная классификация современных информационных угроз.
8. Основные теоретико-прикладные показатели уязвимости защищаемого информационного ресурса.
9. Методологические основы достоверности прогнозирования уязвимости информационных объектов.
10. Развитие подходов к организации информационной безопасности в мире (исторический аспект) с учетом противодействия вызовам социальной инженерии.
11. Методология технологии социальной инженерии.
12. Реальные примеры использования метода социальной инженерии.
13. Социальная инженерии – надстройка на базисе – социологической науке.
14. Методология аналитико-синтетического мышления и знания формализованных процедур (технологий) конструкторско-изобретательской деятельности – факторы, противодействующие воздействию социальной инженерии.
15. Факторы психологии человека, используемые методом социальной инженерии, для достижения цели несанкционированного доступа с конфиденциальной информации.
16. Примеры действий социальных инженеров (синжеров) для получения требуемой информации.
17. «Фрикинг» как средство, используемое социальной инженерией для достижения цели.
18. Действия фрикеров в компьютерных сетях. Навыки социальной инженерии, используемые в новой области.
19. Техники и термины социальной инженерии.
20. Когнитивный базис техники социальной инженерии - особенности принятия решений людьми, их человеческой и социальной психологией.
21. Претекстинг и его использование для получения информации
22. Атаки и по онлайн мессенджерам, например по icq.
23. Фишинг — техника, направленная на жульническое получение конфиденциальной информации, и технология ее использования.
24. Технология использования **«Троянского коня»** и ее психологическая база.
25. **«Дорожное яблоко»** как метод атаки, являющийся адаптацией метода троянского коня. Пример использования.
26. Метод **«Кви про кво»** и технология его реализации.
27. Обратная социальная инженерия цель и метод.
28. Техника обратной социальной инженерии – **диверсия**. Технология ее реализации.
29. Техника обратной социальной инженерии – **реклама**. Технология ее реализации.

30. Защита пользователей от социальной инженерии. Технические и антропогенные средства.

31. Простейшие методы антропогенной защиты. Их общий недостаток.

32. Техническая защита. Основные ее средства: мешающие и заполучить и воспользоваться полученной информацией.

33. Средства защиты, используемые при атаках с помощью электронных писем, как-то e-mail и внутренняя почта сети.

34. Анализ как текста входящих писем (предположительно злоумышленника), так и исходящих (предположительно, цели атаки) по ключевым словам.

35. Возможность написания слов с заменой кириллических букв латиницей для совпадающих символов (a, c, e, o, p, x, y, A, B, C, E, H, K, M, O,P,T,X).

36. Современная постановка целей и задач обеспечения информационной безопасности (переход к интенсивным мерам с учетом психологического аспекта воздействия на пользователя).

37 Определение, принципы и методологический базис формирования основ теории информационной безопасности с учетом возможностей социальной инженерии..

38. Развитие неформальных теоретико-прикладных подходов анализа процессов по информационной безопасности в современных условиях использования социального хакерства.

39.Теоретические основы моделирования современных процессов информационной безопасности в условиях действия социальной инженерии.

40. Теоретико-прикладные модели оценки ущерба от реализации информационных угроз с использованием технологии социальной инженерии.

41. Постановка задачи и основы методологии определения требований к обеспечению информационной безопасности в условиях действия технологии социальной инженерии.

42. Основные параметры безопасности информации (информационного ресурса) с учетом возможных атак со стороны социальной инженерии .

43. Основы методологии оценки основных факторов, влияющих на требуемый уровень обеспечения информационной безопасности.

44. Методологические основы определения весов и классификации возможных условий обеспечения информационной безопасности.

45. Системный подход как основа построения современных комплексов обеспечения информационной безопасности с учетом возможностей социальной инженерии.

46. Определение, типизация и стандартизация современных систем обеспечения информационной безопасности.

47. Современные методологические основы проектирования комплексных систем обеспечения информационной безопасности с учетом защиты от действий технологии социальной инженерии.

48. Методологические основы совокупной оценки функционирования комплексных систем информационной безопасности в условиях возможных атак со стороны социальной инженерии.

49. Перспективы развития межведомственной системы подготовки и переподготовки кадров в области обеспечения информационной безопасности, способных противостоять атакам со стороны социальной инженерии.
50. Типовая модель и виды управления информационной безопасностью (краткосрочное; среднесрочное и долгосрочное) в условия вызовов со стороны социальной инженерии.

Приложение 2

Методические указания для обучающихся по освоению дисциплины

ИНСТИТУТ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

КАФЕДРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСИ

Направление подготовки: 10.04.01 - Информационная безопасность

Направленность (профиль): Менеджмент информационной безопасности

Уровень высшего образования: магистратура

Форма обучения: очная

Королев
2023

1. Общие положения

Цель дисциплины:

Целью изучения дисциплины является углубленное изучение теоретических и прикладных основ социальной инженерии как научной дисциплины, связанной с созданием средств и методов выработки научно обоснованных управленческих решений в области информационной безопасности

Задачи дисциплины:

- раскрытие сущности, целей социальной инженерии (СИ) как метода несанкционированного доступа к информации или системам хранения информации без использования технических средств;
- определение общих методологических подходов построения систем защиты информации с учетом возможных атак с использованием технологии социальной инженерии;
- освоение методических подходов, установления состава защищаемой информации и выявления объектов защиты, подверженных атакам со стороны социального хакерства;
- выявление целесообразных методов определения актуальных информационных угроз и опасных нарушителей (злоумышленников, использующих методы социальной инженерии);
- овладение методами оценки уязвимости защищаемой информации;
- определение методов выявления параметров и структуры систем защиты информации;
- освоение методов установления целесообразного состава мероприятий по защите информации от социального хакерства;
- определение методологических подходов оценки эффективности мер по защите информации от воздействия со стороны атак с использованием методов социальной инженерии.

2. Указания по проведению практических (семинарских) занятий:

Практическое занятие 1. Современные проблемы информационной безопасности Социальная инженерия как технология несанкционированного доступа к информации или системам хранения информации без использования технических средств.

Вид практического занятия: смешанная форма ведения практического занятия.

Образовательные технологии: *групповая дискуссия.*

Исторический аспект развития и становление обеспечения информационной безопасности в мире и в России. Социальная инженерия (СИ) как метод несанкционированного доступа к информации или системам хранения информации без использования технических средств.
Время отведенное на занятие – 4 ч.

Практическое занятие 2. Теоретико-методологические основы оценки уязвимости информационных объектов с учетом возможных воздействий с использованием технологии социальной инженерии

Вид практического занятия: смешанная форма ведения практического занятия.

Образовательные технологии: ***групповая дискуссия.***

Понятие и системная классификация современных информационных угроз, включая социальную инженерию.
Время отведенное на занятие – 4 ч.

Практическое занятие 3. Особенности управления информационной безопасностью в условиях воздействия со стороны социальной инженерии.

Вид практического занятия: смешанная форма ведения практического занятия.

Образовательные технологии: *беседа*

Основные принципы управления современными системами информационной безопасности. Модель управления информационной безопасностью.
Время отведенное на занятие – 4 ч.

Практическое занятие 4. Перспективы развития теории и практики информационной безопасности.

Вид практического занятия: смешанная форма ведения практического занятия.

Образовательные технологии: *практическая работа в группах.*

Анализ состояния и прогноз развития теории информационной безопасности с учетом возрастающего негативного воздействия со стороны социальной инженерии
Время отведенное на занятие – 4 ч.

3. Указания по проведению лабораторного практикума

Не предусмотрено учебным планом

4. Указания по проведению самостоятельной работы студентов

№ п/п	Наименование блока (раздела) дисциплины	Виды СРС
1.	Методы используемые в социальной инженерии	***Подготовка докладов по темам:*** 1. Особенности и методы защиты от фишинг атак. 2. Особенности и методы защиты от реализации угрозы «дорожное яблоко». 3. Особенности и методы защиты от угрозы «троянский конь». *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
2.	Анализ параметров безопасности информации и эффективности ее защиты от проникновения со стороны социальной инженерии.	***Подготовка докладов по темам:*** 1. Социальный инженер в информационной безопасности. 2. Анализ состояния защищенности системы информационной безопасности от социальной инженерии. 3. Основные трудности при защите от социальной инженерии. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
3	Изучение и использование методов защиты пользователей от социальной инженерии. Технические и антропогенные средства	***Подготовка докладов по темам:*** 1. Защита рядовых сотрудников от социальной инженерии. 2. Применение технических средств для защиты от социальной инженерии. 3. Антропогенные источники угроз. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*
4	Особенности управления информационной безопасностью в условиях воздействия со стороны социальной инженерии	***Подготовка докладов по темам:*** 1. Анализ законодательства в области социальной инженерии. 2. Виды воздействия социального инженера. 3. Место социальной инженерии в комплексной системе защиты информации. *Подготовка рефератов, письменная работа, самостоятельное изучение тем.*

5. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

Основная литература:

1.Малинин, В. Н. Статистические методы анализа гидрометеорологической информации : учебник : в 2 томах / В. Н. Малинин. — 2 изд., испр. и доп. — Санкт-Петербург : РГГМУ, 2020 — Том 1 : Первичный анализ и построение эмпирических зависимостей — 2020. — 256 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254123 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

2.Малинин, В. Н. Статистические методы анализа гидрометеорологической информации : учебник : в 2 томах / В. Н. Малинин. — 2 изд., испр. и доп. — Санкт-Петербург : РГГМУ, 2020 — Том 2 : Анализ временных рядов и случайных полей — 2020. — 196 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/254126 (дата обращения: 28.11.2022). — Режим доступа: для авториз. Пользователей

Дополнительная литература:

3.Основы управления информационной безопасностью. Серия «Вопросы управление информационной безопасностью". Выпуск 1 : учебное пособие / А. П. Курило, Н. Г. 3.Милославская, М. Ю. Сенаторов, А. И. Толстой. — Москва : Горячая линия-Телеком, 2012. — 244 с. — ISBN 978-5-9912-0271-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/5178 (дата обращения: 28.11.2022). — Режим доступа: для авториз. пользователей.

6.Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

Интернет-ресурсы:

1.http://www.biblioclub.ru

2.http://znanium.com

7. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю)

- **Перечень программного обеспечения:** MSOffice, PowerPoint.

- **Информационные справочные системы:**

1.Электронные ресурсы образовательной среды Университета.

2.Информационно-справочные системы (Консультант+, Гарант).