Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной
деятельности

_____ С.Т. Князев
«___» _____

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля	Модуль
1157341	Обнаружение, предупреждение и ликвидация последствий компьютерных атак

Екатеринбург

Перечень сведений о рабочей программе модуля	Учетные данные
Образовательная программа 1. Математические методы защиты информации	**Код ОП** 1. 10.05.01/22.01
Направление подготовки 1. Компьютерная безопасность	**Код направления и уровня подготовки** 1. 10.05.01

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Баранский Виталий Анатольевич	доктор физико-математических наук, профессор	Профессор	алгебры и фундаментальной информатики
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Согласовано:

Управление образовательных программ Р.Х. Токарева

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Обнаружение, предупреждение и ликвидация последствий компьютерных атак

1.1. Аннотация содержания модуля

Модуль «Обнаружение, предупреждение и ликвидация последствий компьютерных атак» предполагает получение студентами компетенций по обнаружению, предупреждению и ликвидации последствий компьютерных атак на критическую информационную инфраструктуру Российской Федерации. В модуль входят следующие дисциплины: «Противодействие созданию и распространению вредоносных программ», «Системы обнаружения и предупреждения компьютерных атак», «Реагирование на компьютерные инциденты»

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах
1	Противодействие созданию и распространению вредоносных программ	3
2	Реагирование на компьютерные инциденты	3
3	Системы обнаружения и предупреждения компьютерных атак	2
	ИТОГО по модулю:	8

1.3.Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	Не предусмотрены
Постреквизиты и кореквизиты модуля	Не предусмотрены

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3

Противодействие созданию и распространению вредоносных программ	ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	З-2 - Перечислить основные принципы построения защищенных компьютерных систем З-4 - Классифицировать вредоносные программы и компоненты информационного оружия З-5 - Перечислить признаки опасности и вредоносности компьютерных программ З-6 - Сделать обзор требований по разработке и применению антивирусных средств У-3 - Нейтрализовывать вредоносные программы без вспомогательного аппаратного и программного обеспечения П-1 - Иметь практический опыт проектирования систем защиты информации от несанкционированного доступа
	ПК-1 - Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	З-1 - Описывать принципы построения компьютерных систем и сетей З-7 - Объяснять методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей З-8 - Характеризовать способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности З-12 - Классифицировать организационные меры по защите информации У-3 - Оценивать эффективность защиты информации У-4 - Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации П-1 - Сделать вывод о работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик П-2 - Сделать вывод об эффективности применяемых программно-аппаратных

		средств защиты информации с использованием штатных средств и методик
	ПК-5 - Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	З-1 - Воспроизвести форматы хранения информации в анализируемой компьютерной системе З-2 - Воспроизвести основные форматы файлов, используемые в компьютерных системах З-3 - Воспроизвести особенности хранения конфигурационной и системной информации в компьютерных системах З-4 - Характеризовать уязвимости компьютерных систем и сетей З-11 - Характеризовать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы У-5 - Определять принципы деления программного обеспечения на группы, их специфические свойства и взаимосвязь с компьютерной системой У-7 - Выявлять возможные траектории состояний функционирования системы У-8 - Выявлять несоответствия имеющейся информации ее расположению в системе П-4 - Сделать вывод о характеристиках операционной системы и используемых технологий системного программирования П-5 - Сделать вывод о функциональных свойствах программного обеспечения П-9 - Сделать вывод о групповой принадлежности программного обеспечения
Реагирование на компьютерные инциденты	ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	З-2 - Перечислить основные принципы построения защищенных компьютерных систем З-4 - Классифицировать вредоносные программы и компоненты информационного оружия З-5 - Перечислить признаки опасности и вредоносности компьютерных программ У-1 - Выбирать механизмы защиты, реализованные в программно-аппаратных

		комплексах, с целью построения защищенных компьютерных систем У-4 - Выполнять работы по восстановлению работоспособности информационных систем при реагировании на инциденты информационной безопасности П-2 - Выполнять функции специалиста и эксперта-криминалиста по уголовным делам, возбуждаемым по ст. 273 УК
	ПК-1 - Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	З-1 - Описывать принципы построения компьютерных систем и сетей З-2 - Объяснять методы и методики оценки безопасности программно-аппаратных средств защиты информации З-3 - Описывать принципы построения программно-аппаратных средств защиты информации З-4 - Описывать принципы построения подсистем защиты информации в компьютерных системах З-6 - Объяснять методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации З-7 - Объяснять методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей З-8 - Характеризовать способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности З-12 - Классифицировать организационные меры по защите информации У-1 - Определять параметры функционирования программно-аппаратных средств защиты информации У-2 - Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации У-3 - Оценивать эффективность защиты информации

		У-5 - Анализировать программно-аппаратные средства защиты с целью определения уровня обеспечиваемой ими защищенности и доверия П-1 - Сделать вывод о работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик П-2 - Сделать вывод об эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик П-3 - Сделать вывод об уровне защищенности и доверия программно-аппаратных средств защиты информации
	ПК-5 - Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	З-1 - Воспроизвести форматы хранения информации в анализируемой компьютерной системе З-2 - Воспроизвести основные форматы файлов, используемые в компьютерных системах З-3 - Воспроизвести особенности хранения конфигурационной и системной информации в компьютерных системах З-4 - Характеризовать уязвимости компьютерных систем и сетей З-5 - Описывать технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов З-6 - Воспроизвести порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов З-9 - Характеризовать виды преступлений в сфере компьютерной информации З-11 - Характеризовать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы З-13 - Воспроизвести порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и

		технической экспертизе компьютерных систем З-14 - Объяснять методы проведения расследования компьютерных преступлений, правонарушений и инцидентов З-15 - Объяснять методы анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов З-19 - Классифицировать организационные меры по защите информации У-1 - Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа У-2 - Анализировать структуру механизма возникновения и обстоятельства события У-3 - Определять причину и условия изменения программного обеспечения У-4 - Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику У-7 - Выявлять возможные траектории состояний функционирования системы У-8 - Выявлять несоответствия имеющейся информации ее расположению в системе У-9 - Прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов П-3 - Сделать вывод о причинах, условиях изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы П-4 - Сделать вывод о характеристиках операционной системы и используемых технологий системного программирования П-5 - Сделать вывод о функциональных свойствах программного обеспечения П-6 - Сделать вывод о свойствах алгоритма программного продукта и типах поддерживаемых аппаратных платформ

		П-7 - Сделать вывод о причинах, целях и условиях изменения свойств (состояния) программного обеспечения П-8 - Иметь практический опыт индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы П-10 - Разрабатывать рекомендации по устранению выявленных уязвимостей П-11 - Осуществлять обоснованный выбор индивидуальных признаков программы, позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы П-12 - Сделать вывод о виде, свойствах и состоянии информации (фактическом и первоначальном, в том числе до ее удаления и модификации) в компьютерной системе П-13 - Сделать вывод о причинах и условиях изменения свойств исследуемой информации П-14 - Сделать вывод о механизме, динамике и обстоятельствах события по имеющейся информации на носителе данных или ее копиям П-15 - Сделать вывод об участниках события, их роли, места, условий, при которых была создана, модифицирована или удалена информация П-16 - Сделать вывод о соответствии либо несоответствии действий с информацией специальному регламенту (правилам) П-17 - Подготовить экспертное заключение
Системы обнаружения и предупреждения компьютерных атак	ОПК-16 - Способен проводить мониторинг работоспособности и анализ эффективности средств защиты информации в компьютерных системах и сетях	З-1 - Классифицировать и дать общую характеристику программно-аппаратных средств защиты информации З-2 - Перечислить основные принципы построения защищенных компьютерных систем

		З-3 - Характеризовать особенности реализации методов защиты информации программно-аппаратными средствами З-4 - Классифицировать вредоносные программы и компоненты информационного оружия З-5 - Перечислить признаки опасности и вредоносности компьютерных программ З-6 - Сделать обзор требований по разработке и применению антивирусных средств У-1 - Выбирать механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищенных компьютерных систем У-2 - Оценивать и контролировать эффективность мер защиты разрабатывать компоненты программно-аппаратных комплексов защиты информации П-1 - Иметь практический опыт проектирования систем защиты информации от несанкционированного доступа
	ПК-1 - Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	З-1 - Описывать принципы построения компьютерных систем и сетей З-2 - Объяснять методы и методики оценки безопасности программно-аппаратных средств защиты информации З-3 - Описывать принципы построения программно-аппаратных средств защиты информации З-4 - Описывать принципы построения подсистем защиты информации в компьютерных системах З-5 - Объяснять методы оценки эффективности политики безопасности, реализованной в программно-аппаратных средствах защиты информации З-6 - Объяснять методы и средства оценки корректности и эффективности программных реализаций алгоритмов защиты информации

		З-7 - Объяснять методы анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей З-8 - Характеризовать способы анализа применяемых методов и средств защиты информации на предмет соответствия политике безопасности У-1 - Определять параметры функционирования программно-аппаратных средств защиты информации У-2 - Разрабатывать методики оценки защищенности программно-аппаратных средств защиты информации У-3 - Оценивать эффективность защиты информации У-4 - Применять разработанные методики оценки защищенности программно-аппаратных средств защиты информации П-1 - Сделать вывод о работоспособности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик П-2 - Сделать вывод об эффективности применяемых программно-аппаратных средств защиты информации с использованием штатных средств и методик П-3 - Сделать вывод об уровне защищенности и доверия программно-аппаратных средств защиты информации
	ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	З-3 - Описывать принципы построения систем обнаружения компьютерных атак У-2 - Применять инструментальные средства проведения мониторинга защищенности компьютерных систем У-3 - Применять методы анализа защищенности компьютерных систем и сетей П-1 - Сделать вывод о защищенности компьютерных систем с использованием сканеров безопасности П-2 - Сделать вывод о защищенности сетевых сервисов с использованием средств

		автоматического реагирования на попытки несанкционированного доступа к ресурсам компьютерных систем и сетей
	ПК-5 - Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и инцидентов	З-3 - Воспроизвести особенности хранения конфигурационной и системной информации в компьютерных системах З-4 - Характеризовать уязвимости компьютерных систем и сетей З-5 - Описывать технологии поиска и анализа следов компьютерных преступлений, правонарушений и инцидентов З-6 - Воспроизвести порядок фиксации и документирования следов компьютерных преступлений, правонарушений и инцидентов З-10 - Воспроизвести порядок проведения экспертизы вычислительной техники и носителей компьютерной информации с учетом нормативных правовых актов З-11 - Характеризовать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы З-12 - Объяснять методы анализа систем обеспечения информационной безопасности объектов информатизации на базе компьютерных систем в защищенном исполнении З-13 - Воспроизвести порядок подготовки научно-технических экспертных заключений по результатам выполненных работ по информационно-аналитической и технической экспертизе компьютерных систем З-14 - Объяснять методы проведения расследования компьютерных преступлений, правонарушений и инцидентов З-15 - Объяснять методы анализа остаточной информации и поиска следов для фиксации компьютерных инцидентов

		У-1 - Применять нормативные и правовые акты при проведении криминалистической экспертизы и криминалистического анализа У-2 - Анализировать структуру механизма возникновения и обстоятельства события У-3 - Определять причину и условия изменения программного обеспечения У-4 - Выделять свойства и признаки информации, позволяющие установить ее принадлежность определенному источнику У-7 - Выявлять возможные траектории состояний функционирования системы У-8 - Выявлять несоответствия имеющейся информации ее расположению в системе У-9 - Прогнозировать возможные пути развития новых видов компьютерных преступлений, правонарушений и инцидентов П-3 - Сделать вывод о причинах, условиях изменения свойств (эксплуатационных режимов) аппаратных средств в составе компьютерной системы П-4 - Сделать вывод о характеристиках операционной системы и используемых технологий системного программирования П-5 - Сделать вывод о функциональных свойствах программного обеспечения П-6 - Сделать вывод о свойствах алгоритма программного продукта и типах поддерживаемых аппаратных платформ П-7 - Сделать вывод о причинах, целях и условиях изменения свойств (состояния) программного обеспечения П-8 - Иметь практический опыт индивидуального отождествления оригинала программы (инсталляционной версии) и ее копии на носителях данных компьютерной системы П-10 - Разрабатывать рекомендации по устранению выявленных уязвимостей П-11 - Осуществлять обоснованный выбор индивидуальных признаков программы,

		позволяющих впоследствии идентифицировать ее автора, а также взаимосвязи с информационным обеспечением исследуемой компьютерной системы П-12 - Сделать вывод о виде, свойствах и состоянии информации (фактическом и первоначальном, в том числе до ее удаления и модификации) в компьютерной системе П-13 - Сделать вывод о причинах и условиях изменения свойств исследуемой информации П-14 - Сделать вывод о механизме, динамике и обстоятельствах события по имеющейся информации на носителе данных или ее копиям П-15 - Сделать вывод об участниках события, их роли, места, условий, при которых была создана, модифицирована или удалена информация П-16 - Сделать вывод о соответствии либо несоответствии действий с информацией специальному регламенту (правилам) П-17 - Подготовить экспертное заключение

1.5. Форма обучения

Обучение по дисциплинам модуля может осуществляться в очной формах.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Противодействие созданию и
распространению вредоносных программ

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **Синадский Николай Игоревич, Доцент, УНЦ "Информационная безопасность"**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Классификация вредоносных программ	Понятие об опасных компьютерных программах и данных. Оценка опасностей, связанных с разработкой и использованием программ для ЭВМ. Состав вредоносных программ и команд. Классификация вредоносных программ по основным свойствам и признакам. Основные признаки и возможности компьютерных вирусов, программных закладок, «логических бомб», сетевых «червей», программ «удаленного администрирования» и иных видов опасных программ. Инструментарий, используемый вирмейкерами для создания вредоносных программ. Изучение функциональных возможностей вредоносных программ. Программные воздействия, заведомо приводящие к опасным последствиям. Сущность вредоносных блокирования, удаления, модификации защищаемой компьютерной информации. Программно-управляемые формы несанкционированного копирования информации. Механизмы вирусного заражения. Виды и формы программно-управляемого нарушения работы ЭВМ. Способы несанкционированного запуска опасных программ и команд. Способы внедрения и запуска вредоносных программ. Уязвимые места программного обеспечения автоматизированных систем, способствующие внедрению, запуску, сокрытию, и распространению вредоносных программ. Способы проникновения вредоносных программ в

		локальные и сетевые ЭВМ. Потенциально опасные функции операционной системы. Уязвимости ОС и штатного программного обеспечения, способствующие распространению вредоносных программ. Понятие о случайном и безусловном запуске. Внедрение и запуск программного кода на этапах самотестирования ПЭВМ и загрузки операционной системы. Способы подготовки вредоносных программ к автоматическому запуску. Типичные варианты обмана пользователей, провоцирующих их на запуск неизвестных программ. Внедрение и запуск опасных программ с применением «троянских» оболочек. Возможности программ-«джойнеров».
Р2	Средства и методы защиты от вредоносных компьютерных программ	Виды и возможности антивирусных программ. Меры по реализации изолированной программной среды. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ. Способы выявления деструктивной активности вредоносных программ. Понятие о сигнатуре вредоносного программного кода. Принципы антивирусного сканирования памяти ЭВМ. Понятие о механизмах скрытности вредоносных программ. Демаскирующие признаки вредоносного программного кода. Полиморфизм программного кода. «Stealth»-технологии. Способы сокрытия файловых объектов и процессов на уровне ядра операционной системы. Возможности программ«руткитов». Мониторинг подозрительной активности программ. Статический анализ потенциально опасных программ. Определение истинного типа файла. Просмотр текстовых строк в исполняемых и командных файлах. Рекомендации по дизассемблированию и исследованию программного кода. Динамический анализ опасных программ. Запуск программ в виртуальной среде VMWare. Трассировка программ. Возможности программ типа ExeScope и OllyDebugger. Использование мониторов обращений к стеку сетевых драйверов, файлам и системному реестру. Оформление заключений по результатам исследования неизвестных и опасных программ.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-1 - Способен проводить контрольные проверки работоспособности и эффективности применяемых программно-аппаратных средств защиты информации	У-3 - Оценивать эффективность защиты информации

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Противодействие созданию и распространению вредоносных программ

Электронные ресурсы (издания)

1. Михайлов, А. В.; Компьютерные вирусы и борьба с ними : практическое пособие.; Диалог-МИФИ, Москва; 2012; https://biblioclub.ru/index.php?page=book&id=136089 (Электронное издание)

Печатные издания

1. Духан, Е. И., Синадский, Н. И., Хорьков, Д. А., Гайдамакин, Н. А.; Применение программно-аппаратных средств защиты компьютерной информации : учебное пособие для студентов вузов, обучающихся по специальностям 090102, 090105, 090106.; УГТУ-УПИ, Екатеринбург; 2008 (30 экз.)

2. Касперски, К.; Техника и философия хакерских атак; Солон-Р, Москва; 2001 (3 экз.)

3. Касперски, Касперски К.; Техника и философия хакерских атак - записки мыщ`а; СОЛОН-Пресс, Москва; 2005 (1 экз.)

4. Касперски, Касперски К.; Техника и философия хакерских атак; СОЛОН-Р, Москва; 1999 (1 экз.)

Профессиональные базы данных, информационно-справочные системы

Бакланов, В. В. Противодействие созданию и распространению вредоносных программ / Бакланов В.В. — 2008 .— Курс "Противодействие созданию и распространению вредоносных программ" является специальным курсом для специальности "Компьютерная безопасность". Излагается классификация вредоносных программ. Обсуждаются методы и средства противодействия созданию и распространению вредоносных программ. Включает учебное пособие, программу дисциплины, сборник лабораторных работ, методические указания, экзаменационные материалы, презентации. Предназначен для студентов специальности "Компьютерная безопасность". — в корпоративной сети УрФУ .— <URL:http://study.urfu.ru/view/Aid_view.aspx?AidId=11067>.

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ

http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Противодействие созданию и распространению вредоносных программ

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome
2	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**

3	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Реагирование на компьютерные инциденты

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **Синадский Николай Игоревич, Доцент, УНЦ "Информационная безопасность"**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
    - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Управление инцидентами информационной безопасности	Понятие инцидентов ИБ. Нормативная база в сфере управления инцидентами ИБ. Система управления инцидентами ИБ. Обработка событий и инцидентов ИБ. Реагирование на инциденты ИБ. Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ.
Р2	Сбор и анализ технических данных при реагировании на инциденты	Организация процесса обработки технических данных в рамках реагирования на инциденты ИБ: сбор технических данных с компонентов информационной инфраструктуры; поиск (выделение) из собранных технических данных содержательной (семантической) информации, ее анализ и оформлению; распространение (передача) выделенной и оформленной содержательной (семантической) информации; обеспечение наличия технических данных на этапах создания и эксплуатации информационной инфраструктуры. Сбор и фиксация информации об инцидентах ИБ: способ выявления инцидента ИБ; источник информации об инциденте ИБ; содержание информации об инциденте ИБ, полученной от

		источника; сценарий реализации инцидента ИБ; дата и время выявления инцидента ИБ; состав информационной инфраструктуры, задействованной в реализации инцидента ИБ, в том числе пострадавшей от инцидента ИБ, уровень ее критичности; способы подключения информационной инфраструктуры, задействованной в реализации инцидента ИБ, к сети Интернет или сетям общего пользования; информация об операторе связи и провайдере сети Интернет. Проверка целостности (неизменности) собранных данных, маркирование носителей собранных данных. Криминалистическое копирование (создания образов) энергонезависимых технических данных запоминающих устройств СВТ методом побитового копирования. Копирование содержимого оперативной памяти СВТ и получение данных операционных систем. Копирование протоколов (журналов) регистрации. Копирование сетевого трафика. Поиск (выделение) содержательной (семантической) информации, ее анализ и оформление. Структура протокола обработки технических данных. Технические средства и инструменты для сбора и обработки технических данных: технические средства выполнения криминалистической копии (создания образа) запоминающих устройств и содержимого оперативной памяти СВТ; технические средства получения данных операционных систем о сетевых конфигурациях, о сетевых соединениях, об открытых файлах, о запущенных процессах, об открытых сессиях доступа.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональн	ПК-5 - Способен проводить экспертизы при расследовании компьютерных преступлений, правонарушений и	У-2 - Анализировать структуру механизма возникновения и обстоятельства события

		ой деятельности	инцидентов	

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Реагирование на компьютерные инциденты

Электронные ресурсы (издания)

1. ; Введение в информационную безопасность и защиту информации : учебное пособие.; Новосибирский государственный технический университет, Новосибирск; 2017; https://biblioclub.ru/index.php?page=book&id=575113 (Электронное издание)

Печатные издания

1. Синадский, Н. И., Бакланов, В. В.; Анализ и восстановление данных на носителях с файловой системой NTFS : учеб. пособие.; [ГОУ ВПО УГТУ-УПИ], Екатеринбург; 2007 (70 экз.)

2. Бакланов, В. В.; Введение в информационную безопасность. Направления информационной защиты : курс лекций.; Изд-во Уральского университета, Екатеринбург; 2007 (3 экз.)

3. Расторгуев, С. П.; Основы информационной безопасности : учеб. пособие для студентов вузов, обучающихся по специальностям "Компьютерная безопасность", "Комплексное обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телекоммуникац. систем".; Академия, Москва; 2009 (11 экз.)

Профессиональные базы данных, информационно-справочные системы

Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ

http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Реагирование на компьютерные инциденты

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя	**Не требуется**

		Доска аудиторная	
5	Самостоятельная работа студентов	Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Системы обнаружения и предупреждения компьютерных атак

Рабочая программа дисциплины составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Бакланов Валентин Викторович	кандидат технических наук, доцент	Доцент	Департамент радиоэлектроники и связи
2	Синадский Николай Игоревич	кандидат технических наук, Доцент	Доцент	УНЦ "Информационная безопасность"

Рекомендовано учебно-методическим советом института Естественных наук и математики

Протокол № _7_ от _21.10.2021_ г.

1. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

Авторы:

- **Бакланов Валентин Викторович, Доцент, Департамент радиоэлектроники и связи**
- **Синадский Николай Игоревич, Доцент, УНЦ "Информационная безопасность"**

1.1. Технологии реализации, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология
- Разноуровневое (дифференцированное) обучение
  - Базовый уровень

**Базовый I уровень – сохраняет логику самой науки и позволяет получить упрощенное, но верное и полное представление о предмете дисциплины, требует знание системы понятий, умение решать проблемные ситуации. Освоение данного уровня результатов обучения должно обеспечить формирование запланированных компетенций и позволит обучающемуся на минимальном уровне самостоятельности и ответственности выполнять задания;*
Продвинутый II уровень – углубляет и обогащает базовый уровень как по содержанию, так и по глубине проработки материала дисциплины. Это происходит за счет включения дополнительной информации. Данный уровень требует умения решать проблемы в рамках курса и смежных курсов посредством самостоятельной постановки цели и выбора программы действий. Освоение данного уровня результатов обучения позволит обучающемуся повысить уровень самостоятельности и ответственности до творческого применения знаний и умений.

1.2. Содержание дисциплины

Таблица 1.1

Код раздела, темы	Раздел, тема дисциплины*	Содержание
Р1	Эксплуатация систем обнаружения компьютерных атак	Понятие и классификация атак на компьютерные сети. Основные типы сетевых атак. Средства реализации атак. Механизмы типовых атак, основанных на уязвимостях сетевых протоколов. Атаки на сетевые службы. Атаки с использованием промежуточных узлов и территорий. Технологии обнаружения компьютерных атак и их возможности. Прямые и косвенные признаки атак. Методы обнаружения атак. Сигнатурный анализ и обнаружение аномалий. Классификация систем обнаружения атак (СОА). Сетевые и узловые СОА. Требования, предъявляемые к СОА. Стандартизация в области обнаружения атак. Архитектура СОА. Типовая архитектура СОА в составе сенсора, модуля управления, анализатора, набора протоколов взаимодействия и средства реагирования. Технологии построения СОА. Единая архитектура СОА в рамках концепции CIDF. Формат обмена сообщениями систем обнаружения вторжений IDMEF. Платформа построения систем управления событиями безопасности типа Prelude. Эксплуатация СОА. Варианты размещения СОА. Размещение сенсоров СОА. Реагирование на инциденты. Проблемы, связанные с СОА.

		Технология интеллектуальных многоагентных систем. Понятие агентов защиты. Архитектура многоагентных систем. Агентно-ориентированная система моделирования атак, многоагентная система обнаружения вторжений. Спецификация «системного ядра» многоагентной системы. Проектирование компонентов многоагентной СОА. Разработка сенсоров различного типа. Протоколы информирования о событиях, зафиксированных сенсором. Методологии обнаружения атак: простой поиск по шаблону, поиск по шаблону с сохранением состояния, разбор протоколов, эвристический анализ, обнаружение аномалий, анализ соответствия политике безопасности. Основные математические методы, лежащие в основе обнаружения аномалий, и их реализации в СОА. Модель системы корреляции событий информационной безопасности. Формирование правил обнаружения и сценариев сложных атак. Получение информации об актуальных компьютерных атаках из баз данных уязвимостей компьютерных систем. Структура баз данных CVE и BugTraq. Анализ эффективности применяемых СОА. Организация тестирования СОА. Генерация фонового сетевого трафика. Генерация трафика, содержащего сетевые атаки. Критерии тестирования СОА и их параметры.
Р2	Эксплуатация систем аудита информационной безопасности	Цели и задачи проведения аудита безопасности. Этапы и методы проведения, результаты работ. Нормативно-правовые и организационные основы проведения аудита безопасности компьютерных систем. Международные, государственные и ведомственные стандарты и рекомендации в области информационной безопасности. Анализ адекватности основных документов, регламентирующих применение нормативноправовых и организационных методов обеспечения информационной безопасности. Оценка адекватности модели нарушителя, принятой в организации. Оценка инструкций пользователей и администраторов компьютерных систем. Описание и оценка адекватности организационных методов защиты, применение которых декларируется в политике безопасности. Анализ эффективности применения средств межсетевого экранирования. Анализ конфигурационных файлов. Методика тестирования межсетевых экранов. Определение местоположения защищаемой информации. Анализ технического проекта сети. Описание структуры сети и физического местоположения объектов информатизации, обрабатывающих защищаемую информацию. Описание

		средств и методов защиты, применение которых декларируется в технической документации. Определение структуры информационнотелекоммуникационных сетей. Программные средства анализа топологии вычислительной сети. Определение маршрутов прохождения сетевых пакетов. Обнаружение объектов сети. Построение схемы сети. Выявление телекоммуникационного оборудования. Выявление и построение схемы информационных потоков защищаемой информации. Сетевой мониторинг на основе использования механизма WMI и протоколов ICMP, SNMP и CDP. Применение систем автоматизированного построения схемы сети. Средства и методы выявления уязвимостей в программном обеспечении узлов компьютерной сети. Цели и принципы зондирования узлов сети. Использование коммерческих и свободно распространяемых средств аудита безопасности компьютерных систем. Особенности средств активного аудита. Применение средств анализа защищенности серверов приложений. Применение средств автоматизации комплексного аудита информационной безопасности. Структура и функции комплексных экспертных систем аудита безопасности. Учет структуры аппаратнопрограммных средств объекта информатизации. Ранжирование обнаруженных уязвимостей по степени воздействия на защищаемую информацию. Описание выявленных уязвимостей и определение мер защиты, их устраняющих. Формирование выводов и рекомендаций по устранению обнаруженных недостатков. Проектирование систем анализа защищенности. Обобщенные архитектуры систем активного и пассивного анализа защищенности. Модуль генерирования комплекса сценариев атак. Модуль обновления баз данных уязвимостей компьютерных систем.

1.3. Направление, виды воспитательной деятельности и используемые технологии

Таблица 1.2

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения
Профессиональное воспитание	учебно-исследовательская, научно-исследовательская	Технология формирования уверенности и готовности к самостоятельной успешной профессиональн	ПК-4 - Способен проводить инструментальный мониторинг защищенности компьютерных систем и сетей	У-3 - Применять методы анализа защищенности компьютерных систем и сетей

		ой деятельности		

1.4. Программа дисциплины реализуется на государственном языке Российской Федерации .

2. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Системы обнаружения и предупреждения компьютерных атак

Электронные ресурсы (издания)

1. , Синадский, , Н. И.; Сетевая защита на базе технологий фирмы Cisco Systems. Практический курс : учебное пособие.; Уральский федеральный университет, ЭБС АСВ, Екатеринбург; 2014; http://www.iprbookshop.ru/65983.html (Электронное издание)

2. Голиков, А. М.; Защита информации в инфокоммуникационных системах и сетях : учебное пособие.; Томский государственный университет систем управления и радиоэлектроники, Томск; 2015; https://biblioclub.ru/index.php?page=book&id=480637 (Электронное издание)

Печатные издания

1. Романец, Ю. В., Тимофеев, П. А., Шаньгин, В. Ф.; Защита информации в компьютерных системах и сетях; Радио и связь, Москва; 2001 (20 экз.)

Профессиональные базы данных, информационно-справочные системы

Синадский Н.И. Учебно-методический комплекс дисциплины "Защита информации в компьютерных сетях" [Электронный ресурс] / Н. И. Синадский ; Федер. агентство по образованию, Урал. гос. ун-т им. А. М. Горького, ИОНЦ "Информационная безопасность" [и др.] .— Электрон. дан. (13,3 Мб) .— Екатеринбург : [б. и.], 2008 .— 1 электрон. опт. диск (CD-ROM) .— Загл. с этикетки диска .— <URL:http://elar.urfu.ru/handle/10995/1654>.

Материалы для лиц с ОВЗ

Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

http://www.intuit.ru/ - Национальный открытый университет «ИНТУИТ»

http://www.edu.ru/ - Федеральный портал. Российское образование.

http://study.ustu.ru –портал информационно-образовательных ресурсов УрФУ

http://rtf.ustu.ru - официальный сайт ИРИТ-РтФ

Портал информационно-образовательных ресурсов УрФУ

http://study.ustu.ru/info/default.aspx

Официальный сайт ИРИТ-РтФ http://rtf.ustu.ru

Официальный сайт кафедры ТОР УрФУ http://tor.rtf.ustu.ru

Сайт библиотеки университета http://lib.urfu.ru/

3. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Системы обнаружения и предупреждения компьютерных атак

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения
1	Лекции	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome
2	Практические занятия	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome
3	Консультации	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**
4	Текущий контроль и промежуточная аттестация	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Рабочее место преподавателя Доска аудиторная	**Не требуется**

5	Самостоятельная работа студентов	Мебель аудиторная с количеством рабочих мест в соответствии с количеством студентов Персональные компьютеры по количеству обучающихся Подключение к сети Интернет	Office 365 EDUA3 ShrdSvr ALNG SubsVL MVL PerUsr B Faculty EES Свободное ПО:Google Crome