ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ:
Директор института
Высшая школа электроники и компьютерных наук

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Голлай А. В.
Пользователь: gollaiav
Дата подписания: 23.09.2021

А. В. Голлай

РАБОЧАЯ ПРОГРАММА

дисциплины Б.1.39 Защита информации в сети Интернет
для специальности 10.05.03 Информационная безопасность автоматизированных систем
уровень специалист **тип программы** Специалитет
специализация Информационная безопасность автоматизированных систем критически важных объектов
форма обучения очная
кафедра-разработчик Защита информации

Рабочая программа составлена в соответствии с ФГОС ВО по направлению подготовки 10.05.03 Информационная безопасность автоматизированных систем, утверждённым приказом Минобрнауки от 01.12.2016 № 1509

Зав.кафедрой разработчика,
к.техн.н., доц.

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Соколов А. Н.
Пользователь: sokolovan
Дата подписания: 22.09.2021

А. Н. Соколов

Разработчик программы,
к.юрид.н., доцент

Электронный документ, подписанный ПЭП, хранится в системе электронного документооборота Южно-Уральского государственного университета
ЮУрГУ
СВЕДЕНИЯ О ВЛАДЕЛЬЦЕ ПЭП
Кому выдан: Жернова В. М.
Пользователь: zhernovavm
Дата подписания: 22.09.2021

В. М. Жернова

Челябинск

1. Цели и задачи дисциплины

Подготовка специалистов в сфере защиты информации, передаваемой посредством сети "Интернет", ознакомление с основными понятиями безопасности, правовой защиты информации, подготовка к организации защиты компьютерных систем и сетей от несанкционированного доступа к хранимой информации. Задачи дисциплины: - изучение способов правовой защиты информации, распространяемой посредством сети "Интернет"; - изучение способов организационной защиты информации, распространяемой посредством сети "Интернет"; - изучение способов технической защиты информации, распространяемой посредством сети "Интернет"; - оценка эффективности существующих средств защиты; - изучение механизма организации централизованной антивирусной защиты.

Краткое содержание дисциплины

Дисциплина "Защита информации в сети "Интернет" относится к числу дисциплин вариативной части. Данная дисциплина включает в себя изучение технических, организационных и правовых средств защиты информации и ее носителей, а также позволяет овладеть технологиями защиты информации.

2. Компетенции обучающегося, формируемые в результате освоения дисциплины

Планируемые результаты освоения ОП ВО (компетенции)	Планируемые результаты обучения по дисциплине (ЗУНы)
ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Знать:основные понятия информационной безопасности
	Уметь:разрабатывать политику информационной безопасности
	Владеть:навыками использования универсальных программных продуктов для моделирования и реализации процесса защиты данных при их передаче по каналам связи
ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	Знать:современные методы и средства защиты информации в информационно-телекоммуникационных системах
	Уметь:реализовывать простые информационные технологии, реализующие методы защиты информации
	Владеть:средствами защиты информации в сетях ЭВМ
ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Знать:основные направления защиты информации ; законодательство Российской Федерации в области защиты информации
	Уметь:проводить оценку угроз безопасности объекта информатизации
	Владеть:методами защиты информации
ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	Знать:современные информационные технологии в сфере защиты информации от вредоносного программного обеспечения
	Уметь:

	Владеть:навыками использования универсальных программных продуктов для моделирования и реализации процесса защиты данных при их передаче по каналам связи

3. Место дисциплины в структуре ОП ВО

Перечень предшествующих дисциплин, видов работ учебного плана	Перечень последующих дисциплин, видов работ
Б.1.25 Техническая защита информации, Б.1.31 Информационные технологии	ДВ.1.04.01 Технологии защиты информации в различных отраслях деятельности

Требования к «входным» знаниям, умениям, навыкам студента, необходимым при освоении данной дисциплины и приобретенным в результате освоения предшествующих дисциплин:

Дисциплина	Требования
Б.1.25 Техническая защита информации	знать: возможности технических средств перехвата информации; способы и средства защиты информации от утечки по техническим каналам; уметь анализировать и оценивать угрозы информационной безопасности объекта защиты; владеть навыками выявления угроз безопасности автоматизированным системам
Б.1.31 Информационные технологии	Знать: принципы построения и функционирования современных операционных систем.

4. Объём и виды учебной работы

Общая трудоемкость дисциплины составляет 4 з.е., 144 ч.

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		8
Общая трудоёмкость дисциплины	144	144
Аудиторные занятия:	64	64
Лекции (Л)	32	32
Практические занятия, семинары и (или) другие виды аудиторных занятий (ПЗ)	32	32
Лабораторные работы (ЛР)	0	0
Самостоятельная работа (СРС)	80	80
Самостоятельная работа	80	80
Вид итогового контроля (зачет, диф.зачет, экзамен)	-	экзамен

5. Содержание дисциплины

№ раздела	Наименование разделов дисциплины	Объем аудиторных занятий по видам в часах			
		Всего	Л	ПЗ	ЛР

1	Введение, Политика доступа	20	10	10	0
2	Атаки в сети "Интернет"	16	8	8	0
3	Архитектура браузера	28	14	14	0

5.1. Лекции

№ лекции	№ раздела	Наименование или краткое содержание лекционного занятия	Кол-во часов
1	1	Введение, история WEB, устройство браузера	2
2	1	HTTP-протокол, DNS	2
3	1	HTTP-сессия. Понятия о Cookies	2
4	1	Политика одинакового происхождения. Подделка межсайтовых запросов	2
5	1	Политика одинакового происхождения. Исключения	2
1	2	Межсайтовый скриптинг	2
2	2	Атаки типа XSS	2
3	2	Противодействие атакам XSS	2
4	2	Приватность в сети "Интернет"	2
1	3	Отпечаток браузера (fingerprints)	2
2	3	Атаки типа UI DoS, фишинг и др.	2
3	3	Безопасность пользовательского интерфейса	2
4	3	Протокол защиты транспортного уровня	2
5	3	HSTS HPKP	2
6	3	Веб - Аутентификация	2
7	3	Архитектура браузера	2

5.2. Практические занятия, семинары

№ занятия	№ раздела	Наименование или краткое содержание практического занятия, семинара	Кол-во часов
1	1	Установка git bash	2
2	1	Основы работы с bash	2
3	1	Регулярные выражения. Принципы защиты и нападения	2
4	1	Сбор информации с использованием bash	2
5	1	Обработка данных	2
1	2	Анализ данных	2
2	2	Мониторинг журналов в режиме реального времени	2
3	2	Мониторинг сети	2
4	2	Контроль файловой системы	2
1	3	Добавление записей в журнал	2
2	3	Мониторинг доступности системы	2
3	3	Аудит учетных записей	2
4	3	Разведка, обфускация сценария	2
5	3	Fuzzer, backdor	2
6	3	Пользователи, группы и права доступа	2
7	3	Защита информации с использованием антивирусного программного обеспечения	2

5.3. Лабораторные работы

Не предусмотрены

5.4. Самостоятельная работа студента

Выполнение СРС		
Вид работы и содержание задания	Список литературы (с указанием разделов, глав, страниц)	Кол-во часов
Изучение нормативной базы информационного законодательства	ФЗ № 149 от 27.07.2006, ГК РФ - часть 4, УК РФ - глава 28, Приказ ФСТЭК № 17 от 11.02.2013, ФЗ № 152 от 27.07.2006, ФЗ № 98 от 29.07.2004, ФЗ № 184 от 27.12.2002, ГОСТ Р 51583, ГОСТ Р 51624	20
Подготовка к экзамену	ФЗ № 149 от 27.07.2006, ГК РФ - часть 4, УК РФ - глава 28, Приказ ФСТЭК № 17 от 11.02.2013, ФЗ № 152 от 27.07.2006, ФЗ № 98 от 29.07.2004, ФЗ № 184 от 27.12.2002, ГОСТ Р 51583, ГОСТ Р 51624 Информационное право М.М. Рассолов edslan.54523, Инженерно-техническая защита информации Титов А.А. edslan.4959, Организационная защита информации Аверченков В.И. Рытов М.Ю. edslan.44741 ОСНОВЫ И ОБЕСПЕЧЕНИЕ ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНЫХ СЕТЯХ И В СЕТИ ИНТЕРНЕТ edsclk.16810953	20
Подготовка к аудиторным занятиям	Информационное право М.М. Рассолов edslan.54523, Инженерно-техническая защита информации Титов А.А. edslan.4959, Организационная защита информации Аверченков В.И. Рытов М.Ю. edslan.44741 ОСНОВЫ И ОБЕСПЕЧЕНИЕ ЗАЩИТА ИНФОРМАЦИИ В ГЛОБАЛЬНЫХ СЕТЯХ И В СЕТИ ИНТЕРНЕТ edsclk.16810953	40

6. Инновационные образовательные технологии, используемые в учебном процессе

Инновационные формы учебных занятий	Вид работы (Л, ПЗ, ЛР)	Краткое описание	Кол-во ауд. часов
Интерактивные лекции	Лекции	Лекции с применением мультимедийных технологий, материал которых подводит студентов к возможности самостоятельно отвечать на задаваемые вопросы по текущим темам	16

Собственные инновационные способы и методы, используемые в образовательном процессе

Не предусмотрены

Использование результатов научных исследований, проводимых университетом, в рамках данной дисциплины: нет

7. Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

7.1. Паспорт фонда оценочных средств

Наименование разделов дисциплины	Контролируемая компетенция ЗУНы	Вид контроля (включая текущий)	№№ заданий
Все разделы	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы	Тест	1-10
Все разделы	ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности	Тест	11-20
Все разделы	ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа	Тест	21-30
Все разделы	ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий	Тест	31-33

7.2. Виды контроля, процедуры проведения, критерии оценивания

Вид контроля	Процедуры проведения и оценивания	Критерии оценивания
Тест	Подсчет верных ответов	Отлично: >=25 Хорошо: >=20 Удовлетворительно: >=15 Неудовлетворительно: <15

7.3. Типовые контрольные задания

Вид контроля	Типовые контрольные задания
Тест	ПК-4 способностью разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы 1) Какому типу угроз безопасности информации в первую очередь надо уделять внимание? А) техногенному Б) антропогенному В) стихийному Г) никакому 2) Выберите верное описание угрозы безопасности информации А) УБИj = [нарушитель (источник угрозы); способы реализации угрозы; объекты воздействия; последствия от реализации угрозы]. Б) УБИj = [нарушитель (источник угрозы); уязвимости; объекты воздействия; последствия от реализации угрозы]. В) УБИj = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы;

	объекты воздействия]. Г) УБИj = [нарушитель (источник угрозы); уязвимости; способы реализации угрозы; объекты воздействия; последствия от реализации угрозы]. 3) Какой из перечисленных видов нарушителей имеет наибольший потенциал? А) Конкурирующие организации Б) Специальные службы иностранных государств В) Лица, обеспечивающие функционирование информационных систем Г) Экстремистские группировки 4) Для какого вида нарушителей характерно следующее утверждение: «Имеют возможность создания и применения специальных технических средств для добывания информации (воздействия на информацию или технические средства), распространяющейся в виде физических полей или явлений»? А) Нарушители с базовым (низким) потенциалом Б) Нарушители с базовым повышенным (средним) потенциалом В) Нарушители с высоким потенциалом Г) Для всех 5) Что включает реализация преднамеренных угроз безопасности информации? А) сбор информации об информационной системе, ее структурно- функциональных характеристиках, условиях функционирования; Б) выбор (разработка, приобретение) методов и средств, используемых для реализации угроз безопасности информации в информационной системе с заданными структурно-функциональными характеристиками и условиями функционирования; В) устранение признаков и следов неправомерных действий в информационной системе; Г) Все вышеперечисленное 6) Какова возможная частота реализации угрозы с низкой вероятностью? А) 1 раз в 5 лет Б) 1 раз в год В) 1 раз в месяц Г) 1 раз в день 7) Каким уровнем проектной защищенности информационной системы обладает автономное автоматизированное рабочее место? А) Высокий Б) Средний В) Низкий Г) Нулевой 8) Каким уровнем проектной защищенности информационной системы обладает информационная система, имеющая взаимосвязь с сетями общего пользования? А) Высокий Б) Средний В) Низкий Г) Нулевой 9) Какова возможность реализации угрозы безопасности информации системы с низким уровнем защищенности при наличии у нарушителя высокого потенциала? А) Нулевая Б) Низкая В) Средняя Г) Высокая 10) Что не относится к свойствам безопасности информации? А) Конфиденциальность Б) Целостность В) Актуальность Г) Доступность ПК-10 способностью применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности

	11) Что не относится к функциям межсетевых экранов? А) Обеспечение передачи данных в сеть вне зависимости от установленной политики. Б) Возможность классификации и управления неизвестным трафиком В) Блокирование известных и неизвестных угроз в сетевом трафике Г) Обеспечение одинакового уровня безопасности для всех пользователей и устройств 12) Для реализации каких задач не эффективны аппаратные средства защиты информации? А) проведение специальных исследований технических средств обеспечения производственной деятельности на наличие возможных каналов утечки информации; Б) выявление каналов утечки информации на разных объектах и в помещениях; В) локализация каналов утечки информации; Г) защита информации от копирования 13) Какое преимущество у аппаратных брендмауэров перед программными А) Стоимость Б) Возможность защиты сети изнутри В) Возможность разграничения сегментов локальной сети без выделения подсетей Г) Относительная простота развертывания и использования 14) Как назывался один из первых вирусов современного типа? А) The Greeper Б) The Rabbit В) Никак Г) The Hole 15) Какова основная особенность компьютерных вирусов? А) распространение через Интернет Б) выполнение вредоносных действий В) способность к размножению Г) невозможность уничтожения 16) Существует ли строгая последовательность действий при заражении? А) да Б) нет В) существует общий набор рекомендаций Г) зависит от ОС 17) Что означает термин "файловые вирусы"? А) поражают исполняемые файлы Б) оформлены в виде файлов В) прикрепляются к файлам Г) расширение .exe 18) За счёт чего достигается полиморфизм вирусов? А) за счёт шифрования тела вируса и модификаций программы-расшифровщика Б) за счёт перемешивания его команд В) за счёт удаления некоторых команд Г) за счет многократного копирования 19) Что означает термин "макровирусы"? А) для них характерен большой обьём Б) поражают очень большие файлы В) поражают макросы в электронных документах Г) создают макросы в документах 20) Что понимается под методом независимого от источника информации установления подлинности информации на основе проверки подлинности еѐ внутренней структуры? А) Верификация Б) Аутентификация В) Авторизация Г) Анонимизация ПК-23 способностью формировать комплекс мер (правила, процедуры, методы) для защиты информации ограниченного доступа 21) Что не включает организационная защита информации?

А) Организация работы с персоналом;
Б)Организация внутриобъектового и пропускного режимов и охраны;
В) Разработка внутриорганизационных нормативных правовых актов;
Г) Организация работы с носителями сведений;
22) Расположите в правильном порядке этапе осуществления защиты информации в организации
1.Анализ объекта защиты 2.Выявление угроз 3.Эффективность принятых мер безопасности 4. Определение необходимых мер защиты 5. Реализация мер защиты 6. Осуществление контроля
А) 123456
Б) 213456
В) 124356
Г) 124536
23) Какие меры защиты не входят в состав обязательно реализуемых в информационных системах
А) идентификация и аутентификация субъектов доступа и объектов доступа;
Б) управление доступом субъектов доступа к объектам доступа;
В) защита лиц, имеющих доступ к информационной системе;
Г)обеспечение целостности информационной системы и информации.
24) Что такое политика безопасности?
А) совокупность правил, процедур, практических методов и руководящих принципов в области информационной безопасности, используемых организацией в своей деятельности.
Б) совокупность технических средств защиты информации, используемых организацией в своей деятельности.
В) совокупность нормативных правовых и локальных актов, регламентирующих защиту информации, используемых организацией в своей деятельности.
Г) все выше перечисленное
25) Выберите неверное суждение
А) аудит позволяет оценить текущую безопасность функционирования корпоративной информационной системы
Б) аудит позволяет оценить и спрогнозировать риски, а также управлять их влиянием на бизнес-процессы компании
В) аудит позволяет корректно и обоснованно подойти к вопросу обеспечения безопасности информационных активов компании
Г) аудит позволяет установить ответственных за безопасность лиц
26) Что не относится к атрибутным способом опознавания, используемых системами контроля и управления доступом?
А) паспорт
Б) ключи
В) удостоверение
Г) почерк
27) Кто возглавляет государственную систему защиты информации?
А) ФСТЭК
Б) ФАПСИ
В) ФСБ
Г) Минобороны
28)что не является основанием для отказа в допуске к информации ограниченного доступа (гостайне)?
А) постоянное проживание его самого и (или) его близких родственников за границей и (или) оформление указанными лицами документов для выезда на постоянное жительство в другие государства
Б) выявление в результате проверочных мероприятий действий оформляемого лица, создающих угрозу безопасности Российской Федерации
В) уклонение его от проверочных мероприятий и (или) сообщение им заведомо ложных анкетных данных

	Г) наличие судимости 29)ответственность за создание, использование и распространение вредоносных компьютерных программ А) уголовная Б) дисциплинарная В) административная Г) гражданско-правовая 30) Могут ли АРМ с информационной системой, содержащей государственную тайну, быть подключенными к сетям общего доступа? А) Всегда Б) Никогда В) При наличии антивирусного программного обеспечения Г) при наличии средств защиты, сертифицированными ФСТЭК ОПК-8 способностью к освоению новых образцов программных, технических средств и информационных технологий 31) В чем заключается технология проактивной защиты работы антивируса? А) предотвращение заражения системы пользователя Б) запрет на работу исполняемых файлов В) поиск известного вируса в системе Г) анализ работающих приложений 32) Что позволяет обнаружить эвристический анализ программного кода? А) ранее неизвестные вирусы Б) известные вирусы В) модифицированное вредоносное программное обеспечение Г) все выше перечисленное 33) Что такое сигнатурный анализ? А) выявление характерных идентифицирующих свойств каждого вируса и поиск вирусов при сравнении файлов с выявленными свойствами. Б) Удаление зараженных объектов В) выявление ранее не встречавшихся вирусов Г) анализ работы макросов ФОС ДВ.1.04.01 ЗИ В Интернете.docx

8. Учебно-методическое и информационное обеспечение дисциплины

Печатная учебно-методическая документация

а) основная литература:

Не предусмотрена

б) дополнительная литература:

Не предусмотрена

в) отечественные и зарубежные журналы по дисциплине, имеющиеся в библиотеке:

1. Журнал "Вестник УРФО. Безопасность в информационной сфере"

г) методические указания для студентов по освоению дисциплины:

1. По дисциплине

из них: учебно-методическое обеспечение самостоятельной работы студента:

Электронная учебно-методическая документация

№	Вид литературы	Наименование разработки	Наименование ресурса в электронной форме	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
1	Дополнительная литература	Законодательство РФ	Гарант	ЛокальнаяСеть / Свободный
2	Основная литература	Ворожевич, А. С. Современные информационные технологии и право : монография / А. С. Ворожевич, Е. В. Зайченко, Е. Е. Кирсанова ; под редакцией Е. Б. Лаутс. — Москва : СТАТУТ, 2019. — 288 с. — ISBN 978-5-8354-1578-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130674 (дата обращения: 22.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
3	Основная литература	Диогенес, Ю. Кибербезопасность. стратегия атак и обороны / Ю. Диогенес, Э. Озкайя ; перевод с английского Д. А. Беликова. — Москва : ДМК Пресс, 2020. — 326 с. — ISBN 978-5-97060-709-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/131717 (дата обращения: 22.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
4	Дополнительная литература	Безопасность информационных систем Текст учеб. пособие по направлению 230400 "Информ. системы и технологии" (степень "бакалавр") В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко ; Брян. гос. ун-т им. И. Г. Петровского. 3-е изд., стер. М. Флинта : Наука 2016. Ерохин, В. В.	Электронный каталог ЮУрГУ	Интернет / Авторизованный
5	Дополнительная литература	Ермакова, А. Ю. Методы и средства защиты компьютерной информации : учебное пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2020. — 223 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163844 (дата обращения: 22.09.2021). — Режим доступа: для авториз. пользователей	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный
6	Дополнительная литература	Фот, Ю. Д. Стандарты информационной безопасности : учебное пособие / Ю. Д. Фот. — Оренбург : ОГУ, 2018. — 226 с. — ISBN 978-5-7410-2297-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/159804 (дата обращения: 22.09.2021). — Режим доступа: для авториз. пользователей.	Электронно-библиотечная система издательства Лань	Интернет / Авторизованный

9. Информационные технологии, используемые при осуществлении образовательного процесса

Перечень используемого программного обеспечения:

1. Microsoft-Windows(бессрочно)

Перечень используемых информационных справочных систем:

1. ООО "ГарантУралСервис"-Гарант(бессрочно)
2. -Консультант Плюс(31.07.2017)

10. Материально-техническое обеспечение дисциплины

Вид занятий	№ ауд.	Основное оборудование, стенды, макеты, компьютерная техника, предустановленное программное обеспечение, используемое для различных видов занятий
Лекции	912 (3б)	Мультимедиа
Практические занятия и семинары	913 (3б)	Компьютеры