МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФГБОУ ВО «ИГУ»
Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ
Декан физического факультета
_____ / Н.М. Буднев
“31” 08 2021 г.

Рабочая программа дисциплины

Наименование дисциплины **Б1.В.05 Безопасность информационных систем**

Направление подготовки **10.03.01 Информационная безопасность**

Направленность (профиль) подготовки **Безопасность автоматизированных систем (по отрасли или в сфере профессиональной деятельности)**

Квалификация выпускника **бакалавр**

Форма обучения **очная**

Согласовано с УМК:
физического факультета
Протокол № 30 от «31» августа 2021 г.

Председатель: д.ф.-м.н., профессор
_____ Н.М. Буднев

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 1 от «30» августа 2021 г.

И.о.зав.кафедрой _____ Колесник С.Н.

Иркутск 2021 г.

Содержание

1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

Основные цели и задачи, решаемые в ходе преподавания учебной дисциплины, заключаются в формировании у студентов:

- понимания о технологиях обработки информации и их уязвимых местах;
- навыков проведения анализа угроз и анализа уязвимостей в информационных системах;
- навыка разработки документов исходя из методических материалов ФСТЭК России и ФСБ России;
- навыков использования сертифицированных программных и программно-аппаратных средств защиты информации.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП ВО

Дисциплина «Безопасность информационных систем» базируется на дисциплинах «Информатика», «Теория информации», «Основы информационной безопасности».

3. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Процесс освоения дисциплины направлен на формирование компетенций в соответствии с ФГОС ВО и ОП ВО по направлению подготовки **10.03.01 Информационная безопасность**.

Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-1 Способен разрабатывать организационно-распорядительные документы по защите информации.	Способен проводить анализ уязвимостей системы защиты информации и автоматизированных систем.	Знать: • основные технологии в информационных системах; • регламентирующую документацию ФСТЭК и ФСБ России защиту автоматизированных систем. Уметь: • проводить анализ угроз и анализ уязвимостей для различных автоматизированных и автономных информационных систем. Владеть: • навыками закрытия уязвимостей; • навыками нейтрализации угроз.
ПК-3 Способен внедрять организационные меры по защите информации в автоматизированных системах.		Знать: • основные технологии организации мер по защите информации; Уметь: • реализовывать меры по защите информации в информационных системах Владеть: • навыками закрытия уязвимостей; навыками нейтрализации угроз.

4. СОДЕРЖАНИЕ И СТРУКТУРА ДИСЦИПЛИНЫ

Объем дисциплины составляет 3 зачетных единиц, 108 часов,
Форма промежуточной аттестации: зачет

4.1. Содержание дисциплины, структурированное по темам, с указанием видов учебных занятий и отведенного на них количества академических часов

№ п/н	Раздел дисциплины/тема	Семестр	Всего часов	Из них практическая подготовка обучающихся	Виды учебной работы, включая самостоятельную работу обучающихся, практическую подготовку и трудоемкость (в часах)				Форма текущего контроля успеваемости
					Контактная работа преподавателя с обучающимися			Самостоятельная работа	
					Лекция	Семинар/ Практическое, лабораторное занятие/	Консультация		
1	2	3	4	5	6	7	8	9	10
1	Тема 1.	6	15		4	4		7	Тестовый контроль по теме
2	Тема 2.	6	21		7	7		7	Тестовый контроль по теме
3	Тема 3.	6	21		7	7		7	Тестовый контроль по теме
4	Тема 4.	6	21		7	7		7	Тестовый контроль по теме
5	Тема 5.	6	22		7	7	1	7	Тестовый контроль по теме

4.2. **План внеаудиторной самостоятельной работы обучающихся по дисциплине**

Семестр	Название раздела, темы	Самостоятельная работа обучающихся			Оценочное средство	Учебно-методическое обеспечение самостоятельной работы
		Вид самостоятельной работы	Сроки выполнения	Трудоемкость (час.)		
6	Тема 1-3	Подготовка к контрольной работе №1	1-5 неделя	7	Контрольная работа №1	Список дополнительной литературы
6	Тема 1-3	Контрольная работа №1.	6 неделя	7	Контрольная работа №1	Список дополнительной литературы
6	Тема 1-3	Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.	7 неделя	7	Контрольная работа №1	Список дополнительной литературы
6	Тема 4-5	Подготовка к контрольной работе №2	8-15 неделя	7	Контрольная работа №2	Список дополнительной литературы
6	Тема 4-5	Контрольная работа №2.	16 неделя	7	Контрольная работа №2	Список дополнительной литературы
Общий объем самостоятельной работы по дисциплине (час)				**35**		

4.3. **Содержание учебного материала**

РАЗДЕЛ 1 (Тема 1). ВВЕДЕНИЕ В БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ.

Необходимые понятия информационной безопасности. Основные регламентирующие документы ФСТЭК России и ФСБ России по регулированию защиты информации в РФ

РАЗДЕЛ 2 (Тема 2). УГРОЗЫ НСД НЕПОСРЕДСТВЕННОГО ДОСТУПА И ИХ НЕЙТРАЛИЗАЦИЯ.

Понятие угроз непосредственного доступа. Классификация ФСТЭК России. Классификация ФСБ России. Операционные системы (Windows, Linux) и и механизмы аутентификации. Механизм появления узявимостей. Методы предотвращения эксплуатации уязвимостей НСД непосредственного доступа. Средства защиты информации Классификация средств защиты информации.

РАЗДЕЛ 3 (Тема 3). УГРОЗЫ С ИСПОЛЬЗОВАНИЕМ СЕТЕВЫХ ТЕХНОЛОГИЙ И ИХ НЕЙТРАЛИЗАЦИЯ.

Классификация сетевых угроз. Классификация сетевых уязвимостей. Историческая справка по использованию уязвимостей. Примеры использования уязвимостей. Сетевые службы сервера и клиенты как объекты атаки. Методы предотвращения эксплуатации уязвимостей с использованием сетевых технологий. Средства защиты информации Классификация средств защиты информации. Межсетевые экраны, средства обнаружения вторжения, средства обнаружения таргетированных атак, сканеры анализа уязвимостей.

РАЗДЕЛ 4 (Тема 4). ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ (ФСТЭК РОССИИ).

Правовая область действия регулятора ФСТЭК России. Необходимость формализации защиты информации в правовом поле. Проблемы формализации и их решения. Минимально необходимый и достаточный пакет документов (ФСТЭК России). Модель угроз безопасности. Персональные данные, Государственные информационные системы, конфиденциальная информация.

Раздел 5 (Тема 5). ОРГАНИЗАЦИОННО-РАСПОРЯДИТЕЛЬНЫЕ ДОКУМЕНТЫ (ФСБ РОССИИ).

Правовая область действия регулятора ФСБ России. Минимально необходимый и достаточный пакет документов (ФСБ России), Перечень угроз ФСБ России для информационных систем.

4.3.1. **Перечень семинарских, практических занятий и лабораторных работ**

№ п/п	№ раздела и темы	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)		Оценочные средства	Формируемые компетенции
			Всего часов	Из них практическая подготовка		
1	2	3	4	5	6	7
1.	Раздел 2	Практическая работа №1	4		Тестовый контроль по теме	ПК-1
2.	Раздел 2	Практическая работа №2	7		Тестовый контроль по теме	ПК-1
3.	Раздел 3	Практическая работа №3	7		Тестовый контроль по теме	ПК-1
4.	Раздел 3	Практическая работа №4	7		Тестовый контроль по теме	ПК-3
5.	Раздел 4	Практическая работа №5	7		Тестовый контроль по теме	ПК-3
6.	Раздел 5	Практическая работа №6	7		Тестовый контроль по теме	ПК-3

4.3.2. **Перечень тем (вопросов), выносимых на самостоятельное изучение студентами в рамках самостоятельной работы (СР)**

№ п/п	Тема	Задание	Формируемая компетенция	ИДК
1.	Тема 1	Контрольная работа №1.	ПК-3	Способен проводить анализ уязвимостей системы защиты информации. Способен проводить анализ уязвимостей автоматизированных систем.
2.	Тема 2	Контрольная работа №1.	ПК-1	Способен проводить анализ уязвимостей системы защиты информации. Способен проводить анализ

				уязвимостей автоматизированных систем.
3.	Тема 3	Контрольная работа №1.	ПК-1	Способен проводить анализ уязвимостей системы защиты информации. Способен проводить анализ уязвимостей автоматизированных систем.
4.	Тема 4	Контрольная работа №2.	ПК-3	Способен проводить анализ уязвимостей системы защиты информации. Способен проводить анализ уязвимостей автоматизированных систем.
5.	Тема 5	Контрольная работа №2.	ПК-3	Способен проводить анализ уязвимостей системы защиты информации. Способен проводить анализ уязвимостей автоматизированных систем.

4.4. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Безопасность информационных систем», направленная на углубление и закрепление знаний студента, на развитие практических умений, включает в себя следующие виды работ:

- работа с лекционным материалом;
- подготовка к практическим занятиям;
- подготовка к зачету и экзамену.

Оценка результатов самостоятельной работы организуется как единство двух форм: самоконтроль и контроль со стороны преподавателя.

Каждая лабораторная работа по итогу ее выполнения защищается. В защиту лабораторной работы входят свободно оформленный отчет по проведению работы с зафиксированными ключевыми моментами и результатами работы и вербальное описание хода работы, логики поиска решений и их выполнение.

4.5. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) основная литература

1. 1. Федеральный закон от 27 июля 2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. 2. Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных";
3. 3. Приказ ФСТЭК России от 11 февраля 2013 №17 «Об утверждении требований о защите информации , не составляющей государственную тайну, содержащейся в государственных информационных системах»;

4. Приказ ФСТЭК России от 29 апреля 2021 №77, «Об утверждении порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
5. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
6. Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»
7. Приказ ФСБ РФ №66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации», от 9 февраля 2005 (ПКЗ-2005);

б) дополнительная литература

1. Руководство по эксплуатации Metasloit - https://docs.metasploit.com/;
2. Руководство по эксплуатации Metasloitable 2 https://docs.rapid7.com/metasploit/metasploitable-2;
3. Руководство по эксплуатации Metasloitable 3 - https://github.com/rapid7/metasploitable3.

г) базы данных, информационно-справочные и поисковые системы

1. Банк данных угроз ФСТЭК России (угрозы) - https://bdu.fstec.ru/threat;
2. Банк данных угроз ФСТЭК России (уязвимости) - https://bdu.fstec.ru/vul.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Учебно-лабораторное оборудование:

Компьютерная лаборатория 323б (16 серверов) и лекционная аудитория 225, оснащенные мультимедийными средствами, электронной базой знаний, системой тестирования, выходом в глобальную сеть Интернет. Технические характеристики серверов обеспечивают возможность моделирования необходимого аппаратного обеспечения для работы с современными компьютерными системами хранения и обработки информации.

6.2. Программное обеспечение

1. Oracle VM VirtualBox 5 Бессрочно.
2. Microsoft OfficeProPlus 2013 RUS OLP NL Acdmc. Контракт № 03-013-14 от 08.10.2014.Номер Лицензии Microsoft 45936786. Бессрочно.
3. WinPro10 Rus Upgrd OLP NL Acdmc. Сублицензионный договор № 502 от 03.03.2017 Счет № ФРЗ- 0003367 от 03.03.2017 Акт № 4496 от 03.03.2017 Лицензия № 68203568. Бессрочно.
4. Kaspersky Free (ежегодно обновляемое ПО). Условия использования по ссылке: http://www.kaspersky.ru/free-antivirus/ . Бессрочно.
5. SecretNetStudio 8 (Demo version)
6. Metasploitable 2 (Linux) BSD license
7. Metasploitable 3 (Ubuntu) BSD license
8. Kali Linux, Metasloit 6 GNU GPL.
9. ScanOVAL (ФСТЭК России) Free.

6.3. **Технические и электронные средства:**

В ходе учебного процесса используются технические средства обучения и контроля знаний студентов (презентации, контролирующих программ, демонстрационных установок), использование которых предусмотрено методической концепцией преподавания.

7. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Для достижения планируемых результатов обучения, в дисциплине «Безопасность информационных технологий» используются различные образовательные технологии:

Информационно-развивающие технологии, направленные на формирование системы знаний, запоминание и свободное оперирование ими.

Используется лекционно-семинарский метод, самостоятельное изучение литературы, применение новых информационных технологий для самостоятельного пополнения знаний, включая использование технических и электронных средств информации.

Деятельностные практико-ориентированные технологии, направленные на формирование системы профессиональных практических умений при проведении экспериментальных исследований, обеспечивающих возможность качественно выполнять профессиональную деятельность.

Используется анализ, сравнение методов проведения исследований, выбор метода, в зависимости от объекта исследования в конкретной производственной ситуации и его практическая реализация.

Развивающие проблемно-ориентированные технологии, направленные на формирование и развитие проблемного мышления, мыслительной активности, способности видеть и формулировать проблемы, выбирать способы и средства для их решения. Используются виды проблемного обучения: освещение основных проблем информационной безопасности, учебные дискуссии, коллективная деятельность в группах при выполнении лабораторных работ, решение задач повышенной сложности. При этом используются первые три уровня (из четырех) сложности и самостоятельности: проблемное изложение учебного материала преподавателем; создание преподавателем проблемных ситуаций, а обучаемые вместе с ним включаются в их разрешение; преподаватель создает проблемную ситуацию, а разрешают её обучаемые в ходе самостоятельной деятельности.

Личностно-ориентированные технологии обучения, обеспечивающие в ходе учебного процесса учет различных способностей обучаемых, создание необходимых условий для развития их индивидуальных способностей, развитие активности личности в учебном процессе. Личностно-ориентированные технологии обучения реализуются в результате индивидуального общения преподавателя и студента при защите лабораторных работ, при выполнении домашних индивидуальных заданий, решении задач повышенной сложности, на еженедельных консультациях.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. **Оценочные средства для входного контроля**

Входной контроль (2 варианта, 6-й семестр), представляет собой перечень из 8-10 вопросов и заданий. Входной контроль проводится в письменном виде на первом практическом занятии в течение 15 минут. Проверяется уровень входных знаний.

8.2. **Оценочные средства текущего контроля**

Вопросы к практическим занятиям. Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

8.3. **Оценочные средства для промежуточной аттестации**

(в форме зачета).

Тестовые работы. Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

Демонстрационный вариант тестовой работы

Работа с Metasploit в составе Kali Linux

1. Дано: Сеть из 3 узлов. Узел 1 - Linux (Metasloitable 2), узел 2 - Linux (Metaspoitable 3). узел 3 - Kali Linux.
2. Найти: все уязвимые сервисы связанные с WEB серверами, использую узел 3.
3. Подобрать подходящие эксплоиты с базы с базы Metaspoit для каждой найденной уязвимости.
4. Зафиксировать проведение работы и результат в виде отчета.

ВОПРОСЫ

Вариант 1.

1. С помощью какого ПО можно проводить анализ уязвимостей?

а) Xsdpider;

б) Сканер-ВС;

в) Ревизор сети;

г) Scan Oval

д) Secret Net Studio.

2. Механизм NAT используемый в информационной системе затрудняет или облегчает атаку на информационную систему?

а) затрудняет;

б) облегчает.

3. Burp Suite используется для:

а) анализа уязвимостей Web;

б) анализа уязвимостей SMB;

в) проникновения на изолированные от сети АРМ;

4. Какие функции есть у Framework Metasploit?

а) сканирование портов;

б) вычисление версий сервисов;

в) шифрование данных;

г) эксплуатация уязвимостей

д) подбор паролей.

5. Почему возможна SQL-инъекция?

а) нет фильтрации входных данных к СУБД;

б) WEB сервер содержит уязвимость переполнения буфера.

6. Что такое XSS?

а) тип атаки на веб-системы, заключающийся во внедрении в выдаваемую веб-системой страницу вредоносного кода;

б) тип атаки при которой пользователь попадает на копию запрашиваемого ресурса с измененными данными.

Вариант 2

1. Burp Suite используется для:

а) анализа уязвимостей Web;

б) анализа уязвимостей SMB;

в) проникновения на изолированные от сети АРМ;

2. На каком уровне модели OSI возможны сетевые атаки?

а) на прикладном;

б) на сетевом;

в) на транспортном;

г) на всех перечисленных.

3) Необходим ли анализ уязвимостей при аттестации АРМ ГИС?

а) да;

б) нет;

г) зависит от конкретного ПО.

4) Ошибка переполнения буфера является НДВ?

а) да;

б) нет.

5. Механизм NAT используемый в информационной системе затрудняет или облегчает атаку на информационную систему?

а) затрудняет;

б) облегчает.

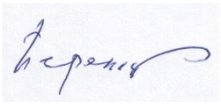
6. Какие методы есть у СОВ?

а) сигнатурные;

б) эвристические.

в) все перечисленные.

Разработчик:



_____доцент_____ _____Ю.Н.Переляев_____

Программа составлена в соответствии с требованиями ФГОС ВО и учитывает рекомендации ПООП по направлению и профилю **10.03.01 Информационная безопасность**.
Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники
«30» августа 2021 г. Протокол № 1

И.О. зав. кафедрой _____ Колесник С.Н.