МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«ИРКУТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФГБОУ ВО «ИГУ»

Кафедра радиофизики и радиоэлектроники

УТВЕРЖДАЮ

Декан _____ Буднев Н.М.

«22» апреля 2020 г.

Рабочая программа дисциплины (модуля)

Наименование дисциплины (модуля) **Б1.В.06 Безопасность информационных технологий**

Направление подготовки 10.03.01 Информационная безопасность

Тип образовательной программы бакалавриат

Направленность (профиль) подготовки №4 Безопасность автоматизированных систем (в сфере профессиональной деятельности)

Квалификация выпускника бакалавр

Форма обучения очная

Согласовано с УМК физического факультета

Протокол № 25 от «21» апреля 2020 г.
Председатель _____ Буднев Н.М.

Рекомендовано кафедрой радиофизики и радиоэлектроники:

Протокол № 8
От «20» марта 2020 г.
И.О.Зав. кафедрой _____ Колесник С.Н.

Иркутск 2020 г.

Содержание

1. Цели и задачи дисциплины (модуля)

Дисциплина «Безопасность информационных технологий», как дисциплина профессионального цикла направлена на достижение следующих целей:

- 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

Дисциплине опирается на знания, полученные в ходе изучения дисциплин «Информатика» и «Теория информации», «Основы информационной безопасности». которые должны быть освоена полностью и студенты должны владеть навыками работы на ПЭВМ.

3. Требования к результатам освоения дисциплины (модуля)

Процесс изучения дисциплины (модуля) направлен на формирование следующих компетенций:

ПК-2 - Способность проводить анализ уязвимостей системы защиты информации и автоматизированных систем.

В результате изучения дисциплины студент должен:

Знать:

- основные технологии в автоматизированных системах;
- регламентирующую документацию ФСТЭК России и ФСБ России защиты автоматизированных систем.

Уметь:

- формализовать поставленную задачу;
- проводить анализ угроз и анализ уязвимостей для различных автоматизированных систем.

Владеть:

- навыками закрытия уязвимостей;
- навыками нейтрализации угроз.

4. Объем дисциплины (модуля) и виды учебной работы

Вид учебной работы	Всего часов / зачетных единиц	Семестры			
		6			
Аудиторные занятия (всего)	64/1,77	64/1,77			
В том числе:	-	-	-	-	-
Лекции	32/0,88	32/0,88			
Практические занятия (ПЗ)	16/0,44	16/0,44			
Семинары (С)					
Лабораторные работы (ЛР)	16/0,44	16/0,44			
КСР					
Самостоятельная работа (всего)	80/2,22	80/2,22			
В том числе:	-	-	-	-	-
Курсовой проект (работа)					
Расчетно-графические работы					
Реферат (при наличии)					
Другие виды самостоятельной работы	80/2,22	80/2,22			
Вид промежуточной аттестации (*зачет, экзамен*)	зачет	зачет			
Контактная работа (всего)	64/1,77	64/1,77			
Общая трудоемкость часы	144	144			
зачетные единицы	4	4			

5. Содержание дисциплины (модуля)

5.1. Содержание разделов и тем дисциплины (модуля). Все разделы и темы нумеруются

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

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 уязвимостей. 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.

5.2. Разделы дисциплины и междисциплинарные связи с обеспечиваемыми (последующими) дисциплинами

№ п/п	Наименование обеспечиваемых (последующих) дисциплин	№№ разделов (тем) данной дисциплины, необходимых для изучения обеспечиваемых (последующих) дисциплин
1	Радиотехнические цепи и сигналы	1-5
2	Защита информации от несанкционированного доступа	1-5
3	Электроника и схемотехника	1-5
4	Операционные системы	1-5
5	Базы данных	1-5
6	Безопасность компьютерных сетей	1-5

5.3. Разделы и темы дисциплин (модулей) и виды занятий

№ п/п	Наименование раздела	Наименование темы	Виды занятий в часах					
			Лекц.	Практ. зан.	Семин	Лаб. зан.	СРС	Всего
1.	***Раздел 1***	Тема 1	4	2		2	16	24
2.	***Раздел 2***	Тема 2	7	2		2	16	27
3.	***Раздел 3***	Тема 3	7	4		4	16	31
4.	***Раздел 4***	Тема 4	7	4		4	16	31
5.	***Раздел 5***	Тема 5	7	4		4	16	31

6. Перечень семинарских, практических занятий и лабораторных работ

№ п/п	№ раздела и темы дисциплины (модуля)	Наименование семинаров, практических и лабораторных работ	Трудоемкость (час.)	Оценочные средства	Формируемые компетенции
1	**2**	**3**	**4**	**5**	**6**
1.	***Раздел 1***	Лабораторная №1	2	Тестовый контроль по теме	ПК-2
2.	***Раздел 2***	Лабораторная №2	2	Тестовый контроль по теме	ПК-2
3.	***Раздел 3***	Лабораторная №3	2	Тестовый контроль по теме	ПК-2
4.	***Раздел 4***	Лабораторная №4	2	Тестовый контроль по теме	ПК-2
5.	***Раздел 5***	Лабораторная №5	4	Тестовый контроль по теме	ПК-2
7.	***Раздел 5***	Лабораторная №6	4	Тестовый контроль по теме	ПК-2

6.1. План самостоятельной работы студентов

№ нед.	Тема	Вид самостоятельной работы	Задание	Рекомендуемая литература	Количество часов
1-7	**1-3**	Подготовка к контрольной работе №1	№1	Учебный сайт	38
8		Контрольная работа №1.		Учебный сайт	1

9		Подведение итогов по контрольной работе №1. Работа над ошибками по контрольной работе №1.		Учебный сайт	1
10-15	**4-5**	Подготовка к контрольной работе №2.	№2	Учебный сайт	38
16		Контрольная работа №2.		Учебный сайт	2

6.2. Методические указания по организации самостоятельной работы студентов

Текущая самостоятельная работа по дисциплине «Безопасность информационных технологий», 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;
- выполнение индивидуальных проектов;
- подготовка к контрольным работам;
- подготовка к зачету.

Творческая проблемно-ориентированная самостоятельная работа по дисциплине «Безопасность информационных технологий», направленная на развитие интеллектуальных умений, общекультурных и профессиональных компетенций, развитие творческого мышления у студентов, включает в себя следующие виды работ по основным проблемам курса:

- поиск, анализ, структурирование информации;
- выполнение графических работ, обработка и анализ данных;
- участие в конференциях, олимпиадах и конкурсах.

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

Самоконтроль зависит от определенных качеств личности, ответственности за результаты своего обучения, заинтересованности в положительной оценке своего труда, материальных и моральных стимулов, от того насколько обучаемый мотивирован в достижении наилучших результатов. Задача преподавателя состоит в том, чтобы создать

условия для выполнения самостоятельной работы (учебно-методическое обеспечение), правильно использовать различные стимулы для реализации этой работы (рейтинговая система), повышать её значимость, и грамотно осуществлять контроль самостоятельной деятельности студента (фонд оценочных средств).

7. Примерная тематика курсовых работ (проектов)

Курсовые работы (проекты) учебным планом не предусмотрены.

8. Учебно-методическое и информационное обеспечение дисциплины (модуля):

а) основная литература

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

9. Материально-техническое обеспечение дисциплины (модуля)

Компьютерная лаборатория 323б (14 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.

10. 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 химических 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 общей и неорганической химии на лекциях, 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.

11. Оценочные средства (ОС):

11.1. Оценочные средства для входного контроля

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

11.2. Оценочные средства текущего контроля

Вопросы к практическим занятиям (5 тем). Представляют собой перечень вопросов, проверяющих знание теоретического лекционного материала и тем, вынесенных на самостоятельную проработку.

11.3. Оценочные средства для промежуточной аттестации

(в форме зачета).

Тестовые работы (2 варианта). Проверяется степень усвоения теоретических и практических знаний, приобретенных умений на репродуктивном и продуктивном уровне.

ВОПРОСЫ

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 эксплойты 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:

преподаватель А.Л. Горбылев

Программа рассмотрена на заседании кафедры радиофизики и радиоэлектроники «20» марта 2020 г.

Протокол № 8 И.О.Зав. кафедрой  Колесник С.Н.