


Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное образовательное учреждение  
высшего образования  
«Сахалинский государственный университет»

Кафедра информатики

УТВЕРЖДАЮ

Руководитель основной профессиональной  
образовательной программы

 Буинцев Д.Н.  
«\_24\_» сентября 2024 г

**РАБОЧАЯ ПРОГРАММА**

Дисциплины

*Б1.В.ДВ.05.02 «Системы анализа уязвимостей ПО»*

Уровень высшего образования

БАКАЛАВРИАТ

Направление подготовки

*10.03.01 Информационная безопасность*

профиль

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

Квалификация

*Бакалавр*

Форма обучения

*очная*

РПД адаптирована для лиц с ограниченными возможностями здоровья и инвалидов

Южно-Сахалинск  
2024

Рабочая программа дисциплины Б1.В.ДВ.05.02 Системы анализа уязвимостей ПО составлена в соответствии с федеральным государственным образовательным стандартом высшего образования (ФГОС ВО) по направлению подготовки 10.03.01 Информационная безопасность.

Программу составил(и):

Вашакидзе Н.С., старший преподаватель кафедры информатики



Рабочая программа дисциплины Б1.В.ДВ.05.02 Системы анализа уязвимостей ПО утверждена на заседании кафедры информатики, протокол № 8 от 19 марта 2024 г.

Исполняющий обязанности  
заведующего кафедрой информатики



Осипов Г.С.

## 1. Цель и задачи дисциплины

### Цель дисциплины

Целями освоения дисциплины Системы анализа уязвимостей ПО является формирование профессиональных компетенций будущих специалистов в области информационной безопасности, формирование у студентов системного и аналитического мышления, овладение принципами организации процесса анализа защищенности автоматизированной системы.

### Задачи дисциплины

Основными задачами изучения дисциплины являются:

- формирование навыков экспертизы качества и надежности реализаций программных и программно-аппаратных средств обеспечения информационной безопасности;
- формирование навыков анализа программных реализаций на предмет наличия уязвимостей;
- использования систем обнаружения вторжений.

## 2. Место дисциплины в структуре образовательной программы

Дисциплина «Системы анализа уязвимостей ПО» относится к обязательной части Блока 1 Дисциплины (модули) (Б1.В.ДВ.05.02) подготовки студентов по направлению подготовки бакалавров 10.03.01 Информационная безопасность.

Пререквизиты дисциплины:

Изучение данной дисциплины базируется на знании следующих дисциплин: Операционные системы, Безопасность операционных систем, Безопасность систем баз данных, Безопасность Web-приложений, Разработка и эксплуатация защищенных автоматизированных систем, Прикладная криптография, Защита персональных данных в организации.

Постреквизиты дисциплины:

Основные положения данной дисциплины выступают опорой для дисциплин: Администрирование и обслуживание компьютерных сетей, Методы и средства криптографической защиты информации, дисциплин по выбору, призваны подготовить к прохождению учебной и производственной практик, к научно-исследовательской работе.

## 3. Формируемые компетенции и индикаторы их достижения по дисциплине

Код компетенции	Содержание компетенции	Код и наименование индикатора достижения компетенции
ПКС-1	Способен проводить формализацию предметной области с целью создания информационной системы в сфере профессиональной деятельности	ПКС-1.1 - Знает критерии оценки эффективности и надежности средств защиты программного обеспечения автоматизированных систем; ПКС-1.2 - Умеет определять параметры настройки программного обеспечения системы защиты информации автоматизированной системы; ПКС-1.3 – Владеет навыками определения параметров настройки программного обеспечения системы защиты информации автоматизированной системы;
ПКС-2	Способен решать задачи профессиональной деятельности с учетом текущего состояния и	ПКС-2.1 - Знает основные меры по защите информации в автоматизированных системах; ПКС-2.2 - Умеет регистрировать и анализировать события, связанные с защитой информации в

	тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации	автоматизированных системах. Умеет регистрировать и анализировать события, связанные с защитой информации в автоматизированных системах; ПКС-2.3 - Владеет навыками использования типовых программных средства резервирования и восстановления информации в автоматизированных системах.
--	---	--

#### 4. Структура и содержание дисциплины (модуля)

##### 4.1. Структура дисциплины (модуля)

Общая трудоемкость дисциплины (модуля) составляет **3** зачетные единицы (**108** академических часов).

Вид работы	Трудоемкость, акад. часов	
	семестр	всего
	7	
<b>Общая трудоемкость</b>	<b>108</b>	<b>108</b>
<b>Контактная работа:</b>	<b>58</b>	<b>58</b>
Лекции (Лек)	24	<b>24</b>
Лабораторные работы (Лаб)	30	<b>30</b>
Контактная работа в период теоретического обучения (КонтТО) ( <i>Проведение текущих консультаций и индивидуальная работа со студентами</i> )	4	<b>4</b>
Контактная работа в период промежуточной аттестации (КонтПА)		<b>0</b>
Промежуточная аттестация – зачет		<b>0</b>
<b>Самостоятельная работа:</b>	<b>50</b>	<b>50</b>
- самостоятельное изучение разделов (перечислить);	0	<b>0</b>
- самоподготовка (проработка и повторение лекционного материала, материала учебников и учебных пособий);	14	<b>14</b>
- подготовка к лабораторным занятиям;	30	<b>30</b>
- подготовка к коллоквиумам;	2	<b>2</b>
- подготовка к промежуточной аттестации и т.п.)	4	<b>4</b>

##### 4.2. Распределение видов работы и их трудоемкости по разделам дисциплины (модуля)

№ п/п	Раздел дисциплины/ темы		Виды учебной работы (в часах)				Формы текущего контроля успеваемости, промежуточной аттестации
			контактная			Самостоятельная работа	
		семестр	Лекции	Практические занятия	Лабораторные занятия		
1.	Тема 1. Понятие защищенности ИС	7	6	0	6	14	Устный опрос по теме лекции. Проверка домашнего задания.
2.	Тема 2. Средства анализа защищенности сетевых сервисов		10	0	12	16	Устный опрос по теме лекции. Проверка домашнего задания.
3.	Тема 3. Средства анализа защищенности web-приложений		8	0	12	14	Устный опрос по теме лекции. Проверка домашнего задания.
	КОЛЛОКВИУМЫ					2	Собеседование

зачет					4	Устный зачет (по билетам)
итого:	68	24	0	30	50	

### 4.3. Содержание разделов дисциплины

#### Тема 1. Понятие защищенности ИС

Понятие защищенности автоматизированной системы. Нормативная база. Методика анализа защищенности. Исходные данные обследуемой ИС. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.

Средства анализа параметров защиты. Классификация методов анализа параметров защиты (Security Benchmarks). Спецификации Security Benchmarks. Спецификации первого уровня для базового (минимального) уровня защиты. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.

#### Тема 2. Средства анализа защищенности сетевых сервисов

Уязвимости сетевых протоколов, служб, сервисов. Классификация средств анализа защищенности сетевых сервисов.

Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС. Функции, методика использования.

#### Тема 3. Средства анализа защищенности web-приложений

Анализ и классификация уязвимостей web-приложений. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC). Комплексная оценка защищенности web-приложения. Принцип «черного ящика» Принцип «серого ящика». Принцип «белого ящика». Инструментальные средства анализа защищенности web-приложения.

### 4.4 Темы и планы лабораторных занятий

#### Лабораторное занятие №1 (6 ч.)

##### Тема Поиск уязвимостей в программной реализации

Вопросы для обсуждения:

1. Понятие защищенности автоматизированной системы.
2. Нормативная база.
3. Методика анализа защищенности. Исходные данные обследуемой ИС.
4. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.
5. Средства анализа параметров защиты.
6. Классификация методов анализа параметров защиты (Security Benchmarks).
7. Спецификации Security Benchmarks.
8. Спецификации первого уровня для базового (минимального) уровня защиты.
9. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.

#### Лабораторное занятие №2 (12 ч.)

##### Тема Средства анализа защищенности сетевых сервисов

Вопросы для обсуждения:

1. Уязвимости сетевых протоколов, служб, сервисов.
2. Классификация средств анализа защищенности сетевых сервисов.
3. Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС.
4. Функции, методика использования.

#### Лабораторное занятие №3 (12 ч.)

## Тема Средства анализа защищенности web-приложений

Вопросы для обсуждения:

1. Анализ и классификация уязвимостей web-приложений.
2. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC).
3. Комплексная оценка защищенности web-приложения.
4. Принцип «черного ящика»
5. Принцип «серого ящика».
6. Принцип «белого ящика».
7. Инструментальные средства анализа защищенности web-приложения.

## 5. Темы дисциплины (модуля) для самостоятельного изучения

Не предусмотрены

## 6. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
	<b>1 семестр</b>		
1.	Тема 1. Понятие защищенности ИС	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
2.	Тема 2. Средства анализа защищенности сетевых сервисов	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторное занятие	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.
3.	Тема 3. Средства анализа защищенности web-приложений	Лекция	Традиционная лекция в ауд. с мультимедиа проектором
		Лабораторные занятия	Лабораторное занятие в компьютерном классе.
		Самостоятельная работа	Изучение материала по теме лекции, подготовка домашнего задания.

## 7. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине (модулю)

Примерные вопросы к зачету

1. Понятие защищенности автоматизированной системы.
2. Нормативная база.
3. Методика анализа защищенности. Исходные данные обследуемой ИС.
4. Методы тестирования системы защиты. Классификация систем и средств анализа защищенности.
5. Средства анализа параметров защиты.

6. Классификация методов анализа параметров защиты (Security Benchmarks).
7. Спецификации Security Benchmarks.
8. Спецификации первого уровня для базового (минимального) уровня защиты.
9. Спецификации второго уровня защиты для систем с повышенными требованиями по безопасности.
10. Уязвимости сетевых протоколов, служб, сервисов.
11. Классификация средств анализа защищенности сетевых сервисов.
12. Сертифицированные средства анализа защищенности: XSpider, MaxPatrol, Ревизор Сети, Сканер-ВС.
13. Функции, методика использования.
14. Анализ и классификация уязвимостей web-приложений.
15. Библиотека документов Open Web Application Security Project (OWASP), проект Web Application Security Consortium (WASC).
16. Комплексная оценка защищенности web-приложения.
17. Принцип «черного ящика»
18. Принцип «серого ящика».
19. Принцип «белого ящика».
20. Инструментальные средства анализа защищенности web-приложения.

## 8. Система оценивания планируемых результатов обучения

### Критерии оценивания

Оценка «зачтено» выставляется:

- студенту глубоко и прочно усвоившему программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагающему, в ответе которого увязывается теория с практикой, он показывает знакомство с литературой, правильно обосновывает и использует рациональные и современные средства решения поставленной проблемы.
- студенту, твердо знающему программный материал, грамотно и по существу, излагающему его, который не допускает существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении поставленной задачи.
- студенту, который знает только основной программный материал, но не усвоил особенностей, допускает в ответе неточности, некорректно формулирует основные законы и правила, затрудняется в выполнении практических задач.

Оценка «не зачтено» выставляется студенту, который не знает значительной части программного материала, допускает в ответе существенные ошибки, с затруднениями практические задания.

Форма контроля	За одну работу		Всего	
	Мин. баллов	Макс. баллов	Мин. баллов	Макс. баллов
Текущий контроль:				
Активная работа на занятии	0,25	0,5	9	18
Выполнение домашнего задания	0,75	0,75	27	27
Выполнение заданий самостоятельной работы	1	3	1	3
коллоквиум	1	3	3	9
Промежуточная аттестация (экзамен)			20	43
<b>Итого за семестр</b> /экзамен			60	100

## 9. Учебно-методическое и информационное обеспечение дисциплины

### 9.1. Основная литература

1. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное

пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2024. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539995>

2. Белов, П. Г. Системный анализ и программно-целевой менеджмент рисков : учебник и практикум для вузов / П. Г. Белов. — Москва : Издательство Юрайт, 2024. — 289 с. — (Высшее образование). — ISBN 978-5-534-04690-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539784>
3. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/538066>

## **9.2. Дополнительная литература**

1. Золотарев В.В., Федорова Н.А. Анализ защищенности автоматизированных систем.- Красноярск, СибГАУ, 2007 – 93 с.
2. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: Учеб. пособие для студ. высш. учеб. заведений / Павел Борисович Хорев. — М.:
3. Издательский центр «Академия», 2005. — 256 с.
4. Белов, П. Г. Системный анализ и программно-целевой менеджмент рисков : учебник и практикум для вузов / П. Г. Белов. — Москва : Издательство Юрайт, 2024. — 289 с. — (Высшее образование). — ISBN 978-5-534-04690-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/539784>
5. Казарин, О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2024. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/543631>

## **9.3. Программное обеспечение**

1. Microsoft Office 2010 Russian Academic OPEN 1 License (бессрочная), (лицензия 49512935);
2. Microsoft Sys Ctr Standard Sngl License/Software Assurance Pack Academic License 2 PROC (бессрочная), (лицензия 60465661)
3. Microsoft Win Home Basic 7 Russian Academic OPEN (бессрочная), (лицензия 61031351),
4. Microsoft Office 2010 Russian Academic OPEN, (бессрочная) (лицензия 61031351),
5. Microsoft Windows Professional 8 Russian Upgrade Academic OPEN (бессрочная), (лицензия 61031351),
6. Microsoft Internet Security&Accel Server Standart Ed 2006 English Academic OPEN, (бессрочная), (лицензия 41684549),
7. Microsoft Office Professional Plus 2010 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
8. Microsoft Windows Server CAL 2008 Russian Academic OPEN, (бессрочная), (лицензия 60939880),
9. Microsoft Windows 10 Pro, 64 bit, Rus, OEM, Операционная система
10. Неисключительное право на использование ПО Kaspersky Endpoint Security для бизнеса – Расширенный Russian Edition.
11. Неисключительное право на использование ПО Kaspersky Security для виртуальных и облачных сред, Server, VirtSvr, License, Education Renewal
12. ABBYYFineReader 11 Professional Edition, (бессрочная), (лицензия AF11-2S1P01-102/AD),



13. Microsoft Volume Licensing Service, (бессрочная), (лицензия 62824441),
14. Microsoft Windows Pro 64bit DOEM, (бессрочная), контракт № 6-ОАЭФ2014 от 05.08.2014
15. Visual Studio Professional
16. «Антиплагиат. ВУЗ». Лицензионный договор № 5044 от 14.05. 2022 года (ежегодное продление);
17. Учебно-методический комплекс «Информационная безопасность» на 20 учебных мест;
18. Учебно-методический комплекс «Безопасность телекоммуникационных систем» на 20 учебных мест.

#### **9.4.Профессиональные базы данных и информационные справочные системы современных информационных технологий**

1. Информационная система «Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии» (<https://habr.com/>)
2. Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки- (<https://github.com/>)
3. База книг и публикаций Электронной библиотеки "Наука и Техника" (<http://www.n-t.ru>)
4. Единое окно доступа к образовательным ресурсам. Раздел Информатика и информационные технологии ([http://window.edu.ru/catalog/?p\\_rubr=2.2.75.6](http://window.edu.ru/catalog/?p_rubr=2.2.75.6))
5. Электронная библиотечная система ZNANIUM.COM (<http://znanium.com/>)
6. Цифровая коллекция электронных версий изданий (учебники, учебные пособия, учебно-методические документы, монографии) по экономическим, естественным, техническим и гуманитарным наукам, сгруппированных по тематическим и целевым признакам.
7. Электронная библиотечная система «BOOK.ru» издательства «КноРус медиа» (<https://www.book.ru/>)
8. Интернет-университет информационных технологий ([www.intuit.ru](http://www.intuit.ru))
9. Онлайн среда разработки приложений ([ideone.com](http://ideone.com))
10. Журнал «КомпьютерПресс» ([www.compress.ru](http://www.compress.ru))
11. Издательство «Открытые системы» ([www.osp.ru](http://www.osp.ru))
12. Издание о высоких технологиях ([www.cnews.ru](http://www.cnews.ru))
13. Справочно-правовая система «Консультант Плюс» (<http://www.consultant.ru>)
14. Polpred.com Обзор СМИ (<http://polpred.com/>)
15. Электронная библиотечная система eLIBRARY.RU (<http://www.elibrary.ru>)
16. Электронная библиотечная система IPRbooks (<http://www.iprbookshop.ru>)
17. Электронная библиотечная система Национальная электронная библиотека (<https://нэб.рф>)
18. Электронная библиотечная система Юрайт (<http://www.biblio-online.ru>)

#### **10.Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов**

Учебные и учебно-методические материалы для самостоятельной работы обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья (ОВЗ) предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации:

##### ***Для слепых и слабовидящих:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих

устройств;

- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

***Для глухих и слабослышащих:***

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

***Для лиц с нарушениями опорно-двигательного аппарата:***

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

***Для слепых и слабовидящих:***

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

***Для глухих и слабослышащих:***

- в печатной форме;
- в форме электронного документа.

***Для обучающихся с нарушениями опорно-двигательного аппарата:***

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

***для слепых и слабовидящих:***

- автоматизированным рабочим местом для людей с нарушением зрения;
- при необходимости обучающимся предоставляется увеличивающее устройство, допускается использование увеличивающих устройств, имеющихся у обучающихся;

***для глухих и слабослышащих:***

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

***для обучающихся с нарушениями опорно-двигательного аппарата:***

- передвижными, регулируемые эргономическими партами СИ-1;

- компьютерной техникой со специальным программным обеспечением.

## **11. Материально-техническое обеспечение дисциплины (модуля)**

Для преподавания и изучения дисциплины используется лекционная аудитория, обеспеченная мультимедиа проектором и сопутствующим оборудованием, интерактивной доской. Используются УМК дисциплины (на бумажном и электронном носителях), фонд научной библиотеки университета, методические и учебно-методические материалы кафедры информатики.

***К рабочей программе прилагаются:***

**Приложение 1** – Фонд оценочных средств для проведения аттестации уровня сформированности компетенций обучающихся по дисциплине (модулю);

**Приложение 2** – Методические указания для обучающихся по освоению дисциплины (модуля).