МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ
Заведующий кафедрой
уравнений в частных производных
и теории вероятностей

А.В. Глушко
25.05.2023г

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.В.10 Безопасность автоматизированных систем управления технологическим процессом

1. Код и наименование направления специальности: 10.05.04 Информационно-аналитические системы безопасности

2. Специализация: Автоматизация информационно-аналитической деятельности

3. Квалификация выпускника: Специалист по защите информации

4. Форма обучения: Очная

5. Кафедра, отвечающая за реализацию дисциплины: Кафедра уравнений в частных производных и теории вероятностей математического факультета

6. Составители программы: Садчиков Павел Валерьевич, кандидат физико-математических наук, доцент

7. Рекомендована: Научно-методическим советом математического факультета Протокол № 0500-06 от 25.05.2023

8. Учебный год: 2026/ 2027 Семестр(ы): 7

9. **Цели и задачи учебной дисциплины**

Цели изучения дисциплины:

формирование знания существующих технологий программирования автоматизированных систем.

Задачи учебной дисциплины:

- приобретение знаний по теории программирования автоматизированных систем управления технологическим процессом (АСУ ТП), устройствах и характеристиках АСУ ТП, способах передачи данных;
- формирование умений и навыков по проектированию и защите ПО для АСУ ТП.

10. Место учебной дисциплины в структуре ООП:

Дисциплина «Безопасность автоматизированных систем управления технологическим процессом» относится к части Блока 1, формируемой участниками образовательных отношений.

Для его успешного освоения необходимы знания и умения, приобретенные в результате обучения по предшествующим (а также параллельно изучаемым) дисциплинам: безопасность операционных систем (операционные системы и их безопасность), безопасность сетей ЭВМ, тактики и техники реализации компьютерных атак.

Дисциплина является предшествующей для курсов «Анализ защищенности информационных систем», «Модели безопасности компьютерных систем».

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями) и индикаторами их достижения:

Код	Название компетенции	Код(ы)	Индикатор(ы)	Планируемые результаты обучения
ПК-1	Способен обеспечивать функционирование средств защиты информации в информационно-аналитических системах	ПК-1.1.	Владеет средствами защиты информации в ИАС	Знать: основные средства защиты информации в ИАС; Уметь: администрировать системы защиты информации от несанкционированного доступа и воздействия; Владеть: навыками администрирования систем обнаружения и предотвращения компьютерных атак.

12. Объем дисциплины в зачетных единицах/час.— __3__/__108___.

Форма промежуточной аттестации: Зачет с оценкой – 7 семестр

13. Трудоемкость по видам учебной работы

Вид учебной работы		Трудоемкость	
		Всего	По семестрам
			7 семестр
Контактная работа		50	50
в том числе:	лекции	34	34
	практические	-	-
	лабораторные	16	16

	курсовая работа	-	-
Самостоятельная работа		58	58
Промежуточная аттестация		-	-
Итого:		**108**	**108**

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК *
1. Лекции			
1.1.	Назначение и состав АСУ ТП	Назначение и состав АСУ ТП	
1.2.	Потенциальная опасность АСУ ТП	Наиболее частые уязвимости АСУ ТП	
		Угрозы для АСУ ТП	
1.3.	Реализация системы информационной безопасности АСУ ТП	Реализация системы информационной безопасности АСУ ТП	
1.4.	Средства и методы защиты информации	Юридическое обоснование информационной безопасности	
		Средства защиты информации	
		Методы защиты информации	
1.5.	Анализ ошибок, видов и последствий отказов	Анализ рисков объектов, управляемых АСУ	
		Расчетные формулы проектирования безопасности АСУ ТП	
2. Лабораторные занятия			
1.1.	Назначение и состав АСУ ТП	Назначение и остав АСУ ТП	
1.2.	Потенциальная опасность АСУ ТП	Наиболее частые уязвимости АСУ ТП	
		Угрозы для АСУ ТП	
1.3.	Реализация системы информационной безопасности АСУ ТП	Реализация системы информационной безопасности АСУ ТП	
1.4.	Средства и методы защиты информации	Юридическое обоснование информационной безопасности	
		Средства защиты информации	
		Методы защиты информации	
1.5.	Анализ ошибок, видов и последствий отказов	Анализ рисков объектов, управляемых АСУ	
		Расчетные формулы проектирования безопасности АСУ ТП	

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Виды занятий (часов)				
		Лекции	Практические	Лабораторные	Самостоятельная работа	Всего
1	Назначение и состав АСУ ТП	4		1	12	17
2	Потенциальная опасность АСУ ТП	6		1	12	19
3	Реализация системы информационной безопасности АСУ ТП	6		2	12	20
4	Средства и методы защиты	12		6	12	30

	информации					
5	Анализ ошибок, видов и последствий отказов	10		6	10	26
	Итого:	34		16	58	108

14. Методические указания для обучающихся по освоению дисциплины:

В процессе преподавания дисциплины используются такие виды учебной работы, как лекции, лабораторные занятия, а также различные виды самостоятельной работы обучающихся. На лекциях рассказывается теоретический материал, на лабораторных занятиях с помощью компьютера решаются задачи по теоретическому материалу, прочитанному на лекциях.

При изучении курса «Безопасность АСУ ТП» обучающимся следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий.

1. После каждой лекции студентам рекомендуется подробно разобрать прочитанный теоретический материал, выучить все определения и формулировки теорем, разобрать примеры, решенные на лекции. Перед следующей лекцией обязательно повторить материал предыдущей лекции.

2. Перед лабораторным занятием обязательно повторить лекционный материал.

3. При подготовке к лабораторным занятиям повторить основные понятия по темам, изучить примеры.

4. Выбрать время для работы с литературой по дисциплине в библиотеке.

5. Кроме обычного курса в системе «Электронный университет», все необходимые для усвоения курса материалы размещены также на кафедральном сайте http//:www.kuchp.ru .

Освоение дисциплины предполагает не только обязательное посещение обучающимся аудиторных занятий (лекций и лабораторных занятий) и активную работу на них, но и самостоятельную учебную деятельность в семестрах, на которую отводится 58 часов.

Самостоятельная учебная деятельность студентов по дисциплине предполагает изучение рекомендуемой преподавателем литературы по вопросам лекционных и лабораторных занятий (приведены выше), самостоятельное освоение понятийного аппарата и подготовку к текущим аттестациям (контрольным работам и выполнению домашних заданий) (примеры см. ниже).

Вопросы лекционных и практических занятий обсуждаются на занятиях в виде устного опроса – индивидуального и фронтального. При подготовке к лекционным и лабораторным занятиям обучающимся важно помнить, что их задача, отвечая на основные вопросы плана занятия и дополнительные вопросы преподавателя, показать свои знания и кругозор, умение логически построить ответ, владение математическим аппаратом и иные коммуникативные навыки, умение отстаивать свою профессиональную позицию. В ходе устного опроса выявляются детали, которые по каким-то причинам оказались недостаточно осмысленными студентами в ходе учебных занятий. Тем самым опрос выполняет важнейшие обучающую, развивающую и корректирующую функции, позволяет студентам учесть недоработки и избежать их при подготовке к промежуточным аттестациям (7 семестр – зачет с оценкой)

Все выполняемые студентами самостоятельно задания (выполнение контрольной работы и домашних заданий) подлежат последующей проверке преподавателем. Результаты текущих аттестаций учитываются преподавателем при проведении промежуточной аттестации (7 семестр – зачет с оценкой).

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

а) основная литература:

№ п/п	Источник
1	Голуб В.А. Информационная безопасность телекоммуникационных систем : Учебное пособие .— Воронеж : Студия ИАН, 2002 .— 157,[1] с. — <URL:http://www.lib.vsu.ru/elib/books/b102829.djvu>.

б) дополнительная литература:

№ п/п	Источник
1	Абрамов И.В. Информационно-технологическое моделирование и Business Studio [Электронный ресурс] : учебно-методическое пособие :] / И.В. Абрамов, М.Г. Матвеев ; Воронеж. гос. ун-т .— Электрон. текстовые дан. — Воронеж : Издательский дом ВГУ, 2017 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/m17-179.pdf>.

в) информационные электронно-образовательные ресурсы (официальные ресурсы интернет)**:**

№ п/п	Ресурс
1	*http://eqworld.ipmnet.ru – интернет-портал, посвященный уравнениям и методам их решений*
2	*http://www.lib.vsu.ru - электронный каталог ЗНБ ВГУ*
3	*http://www.kuchp.ru – электронный сайт кафедры уравнений в частных производных и теории вероятностей, на котором размещены методические издания*
4	*ЭБС «Университетская библиотека онлайн»*
5	*Электронный курс* Курс: Теория вероятностей копия 2 (vsu.ru)

16. Перечень учебно-методического обеспечения для самостоятельной работы:

№ п/п	Источник
1	Голуб В.А.. Информационная безопасность компьютерных систем. Защита целостности информации : учебное пособие для вузов / В.А. Голуб ; Воронеж. гос. ун-т .— Воронеж : ЛОП ВГУ, 2006 .— 31 с. — Библиогр.: с. 30 .— <URL:http://www.lib.vsu.ru/elib/texts/method/vsu/may07046.pdf>.

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ, электронное обучение (ЭО), смешанное обучение):

При реализации дисциплины используются следующие образовательные технологии: логическое построение дисциплины, установление межпредметных связей, обозначение теоретического и практического компонентов в учебном материале, актуализация личного и учебно-профессионального опыта обучающихся, включение элементов дистанционных образовательных технологий.

Дисциплина может реализовываться с применением дистанционных образовательных технологий, например, на платформе «Электронный университет ВГУ» ().

Перечень необходимого программного обеспечения: операционная система Windows или Linex, Microsoft, Windows Office, LibreOffice 5*, Calc, Math,* браузер Mozilla Firefox, Opera или Internet.

18. Материально-техническое обеспечение дисциплины:

Специализированная мебель, маркерная доска, персональные компьютеры

Компьютерный класс

(394018, г. Воронеж, площадь Университетская, д. 1, пом. I)

Учебная аудитория для проведения занятий лекционного и семинарского типа, текущего контроля и промежуточной аттестации; специализированная мебель

Ubuntu (бесплатное и/или свободное ПО, лицензия: https://ubuntu.com/download/desktop)
Visual Studio Community (бесплатное и/или свободное ПО, лицензия https://visualstudio.microsoft.com/ru/vs/community/)

LibreOffice (GNU Lesser General Public License (LGPL), бесплатное и/или свободное ПО, лицензия: https://ru.libreoffice.org/about-us/license/)

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Наименование раздела дисциплины (модуля)	Компетенция(и)	Индикатор(ы) достижения компетенции	Оценочные средства
1	Назначение и состав АСУ ТП	ПК 1	ПК-1.1	Опрос
2	Потенциальная опасность АСУ ТП	ПК 1	ПК-1.1	Опрос
3	Реализация системы информационной безопасности АСУ ТП	ПК 1	ПК-1.1	Опрос
4	Средства и методы защиты информации	ПК 1	ПК-1.1	Контрольная работа №1
5	Анализ ошибок, видов и последствий отказов	ПК 1	ПК-1.1	Контрольная работа №2
Промежуточная аттестация Форма контроля –зачет с оценкой				Перечень вопросов к зачету

20. Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1. Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Примерный перечень вопросов для устного опроса

Назначение и состав АСУ ТП
Наиболее частые уязвимости АСУ ТП
Угрозы для АСУ ТП
Реализация системы информационной безопасности АСУ ТП
Юридическое обоснование информационной безопасности
Средства защиты информации
Методы защиты информации
Анализ рисков объектов, управляемых АСУ
Расчетные формулы проектирования безопасности АСУ ТП

Текущий контроль представляет собой проверку усвоения учебного материала теоретического и практического характера, регулярно осуществляемую на занятиях.

Цель текущего контроля: определение уровня сформированности профессиональных компетенций, знаний и навыков деятельности в области знаний, излагаемых в курсе.

Задачи текущего контроля: провести оценивание

1. уровня освоения теоретических и практических понятий, научных основ профессиональной деятельности;

2. степени готовности обучающегося применять теоретические и практические

знания и профессионально значимую информацию, сформированности когнитивных умений.

3. приобретенных умений, профессионально значимых для профессиональной деятельности.

Текущий контроль предназначен для проверки хода и качества формирования компетенций, стимулирования учебной работы обучаемых и совершенствования методики освоения новых знаний. Он обеспечивается проведением контрольных работ.

В ходе контрольной работы №1 обучающемуся выдается КИМ с практическим перечнем из двух заданий и предлагается решить данные задания. В ходе выполнения заданий можно пользоваться любой литературой, ограничение по времени 90 минут.

В ходе контрольной работы №2 обучающемуся выдается КИМ с практическим перечнем из двух заданий и предлагается решить данные задания. В ходе выполнения заданий можно пользоваться любой литературой, ограничение по времени 90 минут.

Если текущая аттестация проводится в дистанционном формате, то обучающийся должен иметь компьютер и доступ в систему «Электронный университет». Если у обучающегося отсутствует необходимое оборудование или доступ в систему, то он обязан сообщить преподавателю об этом за 2 рабочих дня. На контрольную работу в дистанционном режиме отводится ограничение по времени 90 минут

При текущем контроле уровень освоения учебной дисциплины и степень сформированности компетенции определяются оценками «неудовлетворительно». «удовлетворительно», «хорошо» и «отлично», которые формируются следующим образом:

Контрольная работа №1 – «удовлетворительно» за одну правильно решенную задачу, «хорошо» за две правильно решенные задачи, «отлично» за три правильно решенные задачи.

Контрольная работа №2 – «удовлетворительно» за одну правильно решенную задачу, «хорошо» за две правильно решенные задачи, «отлично» за три правильно решенные задачи.

20.2. Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Перечень теоретических вопросов:

Назначение и состав АСУ ТП
Наиболее частые уязвимости АСУ ТП
Угрозы для АСУ ТП
Реализация системы информационной безопасности АСУ ТП
Юридическое обоснование информационной безопасности
Средства защиты информации
Методы защиты информации
Анализ рисков объектов, управляемых АСУ
Расчетные формулы проектирования безопасности АСУ ТП

Промежуточная аттестация предназначена для определения уровня освоения всего объема учебной дисциплины. Промежуточная аттестация по дисциплине «Безопасность автоматизированных систем управления технологическим процессом» проводится в форме зачета с оценкой.

Промежуточная аттестация, как правило, осуществляется в конце семестра. Результаты текущей аттестации обучающегося по решению кафедры могут быть учтены при проведении промежуточной аттестации. При несогласии студента, ему дается возможность пройти промежуточную аттестацию (без учета его текущих аттестаций) на общих основаниях.

При проведении зачета учитываются результаты опросов и контрольных работ.

Зачет проходит в форме индивидуального опроса по перечню вопросов к зачету. Для получения оценки «отлично» на зачете в конце 7 семестра у обучающегося должны иметься оценки «отлично» по контрольным работам. Для получения оценки «хорошо» на зачете у обучающегося должны иметься оценки не ниже «хорошо» по обеим контрольным работам.

Требования к выполнению заданий, шкалы и критерии оценивания.

Собеседование по билетам к зачету:

Критерии оценивания компетенций	Шкала оценок
Обучающийся не владеет основами учебно-программного материала, обнаружил пробелы в знаниях основного учебно-программного материала, допустил принципиальные ошибки в выполнении предусмотренных программой заданий	«Неудовлетворительно»
Обучающийся владеет знаниями основного учебно-программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности, справился с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой. Оценка "удовлетворительно" выставляется обучающимся, допустившим погрешности в ответе на экзамене и при выполнении экзаменационных заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя. Оценка «удовлетворительно» выставляется, если студент знает все определения и формулировки утверждений по контрольно-измерительному материалу.	"Удовлетворительно"
Обучающийся полностью владеет знаниями учебно-программного материала, успешно выполнил предусмотренные в программе задания, усвоил основную литературу, рекомендованную в программе. Оценка "хорошо" выставляется обучающимся, показавшим систематический характер знаний по дисциплине и способным к их самостоятельному применению в практической деятельности. Оценка «хорошо» выставляется обучающемуся, если он правильно и в полном объеме ответил не менее, чем на 75% вопросов билета	"Хорошо"
Оценка «отлично» выставляется обучающимся, обнаружившим всестороннее, систематическое и глубокое знание учебно-программного материала, умение свободно выполнять задания, предусмотренные программой, усвоившим основную программу и знакомым с дополнительной литературой, рекомендованной программой. Оценка "отлично" выставляется обучающимся, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании учебно-программного материала. Оценка «отлично» выставляется, если обучающийся в полном объеме и правильно ответил на все вопросы контрольно-измерительного материала	"Отлично"

20.3 Фонд оценочных средств сформированности компетенций студентов, рекомендуемый для проведения диагностических работ

ПК-1 Способен обеспечивать функционирование средств защиты информации в информационно-аналитических системах

ПК-1.1. Владеет средствами защиты информации в ИАС

Знать: основные средства защиты информации в ИАС;

Уметь: администрировать системы защиты информации от несанкционированного доступа и воздействия;

Владеть: навыками администрирования систем обнаружения и предотвращения компьютерных атак.

Тесты

№	Вопрос	Варианты ответов	Правильный ответ
1	Сетевой атакой, цель которой заключается в выявлении работающих в сети служб, открытых портов, активных сетевых сервисов, используемых протоколов, является:	А) Анализ сетевого трафика. Б) Сканирование сети. В) Подмена доверенного объекта сети. Г) Атака «отказ в обслуживании».	А) Анализ сетевого трафика.
2	Сетевой атакой, цель которой заключается в создании таких условий, при которых легитимные пользователи системы не могут получить доступ к предоставляемым системой ресурсам, либо этот доступ затруднён, является:	А) Анализ сетевого трафика. Б) Сканирование сети. В) Подмена доверенного объекта сети. Г) Атака «отказ в обслуживании».	Г) Атака «отказ в обслуживании».
3	Сетевой атакой, в результате реализации которой нарушитель получает возможность перехватывать и передавать в канал связи сетевой трафик, является:	А) Атака «Человек по-середине». Б) Сканирование сети. В) Подмена доверенного объекта сети. Г) Атака «отказ в обслуживании».	А) Атака «Человек по-середине».
4	Атаки, нарушающие работу протоколов маршрутизации, реализуются на:	А) Физическом уровне. Б) Канальном уровне. В) Сетевом уровне. Г) Прикладном уровне.	Г) Прикладном уровне.
5	Атака переполнения таблицы коммутации реализуется на:	А) Физическом уровне. Б) Канальном уровне. В) Сетевом уровне. Г) Прикладном уровне.	Б) Канальном уровне.
6	Сканирование портов осуществляется на:	А) Канальном уровне. Б) Сетевом уровне. В) Транспортном уровне. Г) Прикладном уровне.	В) Транспортном уровне.
7	Для восстановления прообраза по известному хеш-значению не	А) Брутфорс-атака.	В) Обратное

	может использоваться:	Б) Радужные таблицы. В) Обратное преобразование. Г) Перебор по словарю.	преобразование.
8	Аббревиатура APT означает:	-	Целевая атака
9	Вид интернет-мошенничества и компьютерных атак, цель которых получить идентификационные данные пользователей или иную конфиденциальную информацию за счет создания ложных интерфейсов, писем и иных доверенных объектов, называется:	-	Фишинг
10	База данных (матрица), содержащая информацию о тактиках и техниках компьютерных атак, называется:	-	MITRE ATT&CK

№	Вопрос	Варианты ответов	Правильный ответ
11	Непосредственно для защиты информации от утечек используются:	А) DLP-системы. Б) SIEM-системы. В) IPS-системы. Г) IDS-системы.	А) DLP-системы.
12	Непосредственно для управление информацией и событиями в системе безопасности используются:	А) DLP-системы. Б) SIEM-системы. В) IPS-системы. Г) IDS-системы.	Б) SIEM-системы.
13	Непосредственно для предупреждения компьютерных атак используются:	А) DLP-системы. Б) SIEM-системы. В) IPS-системы. Г) IDS-системы.	В) IPS-системы.
14	Методом предотвращения вторжений, основанным на их предварительном обнаружении по набору известных признаков, является:	А) Сигнатурный анализ. Б) Эвристический анализ. В) Поведенческий анализ. Г) Анализ сетевого трафика.	А) Сигнатурный анализ.
15	Непосредственно для защиты БД SQL может использоваться:	А) HIDS. Б) PIDS.	Г) APIDS.

		В) VMIDS. Г) APIDS.	
16	Непосредственно для защиты виртуальных машин может использоваться:	А) HIDS. Б) PIDS. В) VMIDS. Г) APIDS.	В) VMIDS.
17	Непосредственно для защиты отдельных сетевых хостов может использоваться:	А) HIDS. Б) PIDS. В) VMIDS. Г) APIDS.	А) HIDS.
18	Целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и (или) создания угрозы безопасности обрабатываемой таким ресурсом информации называется:	-	Компьютерной атакой
19	Для предотвращения компьютерных атак используются:	-	IPS-системы
20	Для обнаружения компьютерных атак используются:	-	IPS-системы

Критерии и шкалы оценивания заданий ФОС:

1) Задания закрытого типа (выбор одного варианта ответа, верно/неверно):

- 1 балл – указан верный ответ;
- 0 баллов – указан неверный ответ.

2) Задания закрытого типа (множественный выбор):

- 2 балла – указаны все верные ответы;
- 0 баллов — указан хотя бы один неверный ответ.

3) Задания закрытого типа (на соответствие):

- 2 балла – все соответствия определены верно;
- 0 баллов – хотя бы одно сопоставление определено неверно.

4) Задания открытого типа (короткий текст):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

5) Задания открытого типа (число):

- 2 балла – указан верный ответ;
- 0 баллов – указан неверный ответ.

Задания раздела 20.3 рекомендуются к использованию при проведении диагностических работ с целью оценки остаточных результатов освоения данной дисциплины (знаний, умений, навыков).