

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ЛУГАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ ВЛАДИМИРА ДАЛЯ»

Факультет компьютерных систем и информационных технологий
Кафедра автоматизации и компьютерно-интегрированных технологий

УТВЕРЖДАЮ

Декан факультета компьютерных
систем и информационных технологий

Кочевский А. А.

04 _____ 2023 г.



РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Безопасность автоматизированных систем»

по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств

профиль подготовки «Компьютерные и специализированные системы автоматизации производств»

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Безопасность автоматизированных систем» по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств. – 13 с.

Рабочая программа учебной дисциплины «Безопасность автоматизированных систем» составлена на основе федерального государственного образовательного стандарта высшего образования по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств, утвержденного приказом Министерства образования и науки Российской Федерации от 09.08.2021 года № 730 (с изменениями и дополнениями), зарегистрированного в Министерстве юстиции Российской Федерации 03 сентября 2021 года за № 64887, учебного плана по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств, (профиль «Компьютерные и специализированные системы автоматизации производств») и Положения о рабочей программе учебной дисциплины в ФГБОУ ВО «ЛГУ им. В. Даля».

СОСТАВИТЕЛЬ

канд. техн. наук, доцент, доцент кафедры автоматизации и компьютерно-интегрированных технологий Воронов А. Э.

Рабочая программа дисциплины утверждена на заседании кафедры автоматизации и компьютерно-интегрированных технологий
18 апреля 2023 г., протокол № 17
Заведующий кафедрой автоматизации и компьютерно-интегрированных технологий _____ Колесников А. В.

Переутверждена: «___» _____ 20__ г., протокол № _____

Согласована:

Декан факультета компьютерных систем и информационных технологий _____ Кочевский А. А.

Рекомендована на заседании учебно-методической комиссии факультета компьютерных систем и информационных технологий
19 апреля 2023 г., протокол № 8

Председатель учебно-методической комиссии факультета компьютерных систем и информационных технологий _____ Ветрова Н. Н.

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Цель изучения дисциплины – сформировать представление о комплексе мер обеспечения безопасности информации в автоматизированных системах на всех уровнях.

Задачи:

- изучить основные угрозы информационной безопасности;
- изучить источники угроз, виды и причины возникновения уязвимостей;
- изучить основные алгоритмы защиты хранимой и передаваемой информации в автоматизированных системах.

2. Место дисциплины в структуре ООП ВО

Дисциплина «Безопасность автоматизированных систем» входит в часть учебного плана, формируемую участниками образовательных отношений, по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств.

Основывается на базе дисциплин: «Программирование и основы алгоритмизации систем управления», «Web технологии в системах автоматизации», «Технология программирования процессов автоматического управления».

Является основой для подготовки ВКР бакалавра, последующей профессиональной деятельности.

3. Требования к результатам освоения содержания дисциплины

Студенты, завершившие изучение дисциплины «Безопасность автоматизированных систем», должны

знать: методику разработки концепции автоматизированных систем управления технологическими процессами; правила осуществления авторского надзора за изготовлением, испытанием, внедрением и эксплуатацией автоматизированных систем управления технологическими процессами, а также методику обеспечения защиты авторских прав на решения, содержащиеся в разрабатываемых проектах;

уметь: разрабатывать концепции автоматизированных систем управления технологическими процессами; осуществлять авторский надзор за процессом изготовления автоматизированных систем управления технологическими процессами и обеспечивать мероприятия по защите авторских прав на решения, содержащиеся в разрабатываемых проектах;

владеть: навыками разработки концепции автоматизированных систем управления технологическими процессами; навыками осуществления авторского надзора за процессом изготовления автоматизированных систем управления технологическими процессами и обеспечения мероприятий по защите авторских прав на решения, содержащиеся в разрабатываемых проектах.

Перечисленные результаты образования являются основой для формирования следующих компетенций (в соответствии с ФГОС ВО и требованиями к результатам освоения основной профессиональной образовательной программы (ОПОП ВО):

профессиональных:

ПК-1 способен проводить анализ технологических процессов механосборочного производства с целью выявления операций, подлежащих автоматизации и механизации

ПК-4 способен осуществлять подготовку к выпуску проекта автоматизированной системы управления технологическими процессами

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (з.е.)		
	Очная форма	Очно-заочная форма	Заочная форма
Объем учебной дисциплины (всего)	108 (3 з.е.)	-	108 (3 з.е.)
Обязательная аудиторная учебная нагрузка дисциплины (всего)	70	-	14
в том числе:			
Лекции	28	-	6
Семинарские занятия	-	-	-
Практические занятия	14	-	2
Лабораторные работы	28	-	6
Курсовая работа (курсовой проект)	-	-	-
Индивидуальное задание	18	-	18
Самостоятельная работа студента (всего)	38	-	94
Форма аттестации	зачёт	-	зачёт

4.2. Содержание разделов дисциплины

Тема 1. Введение в безопасность автоматизированных систем
Основные понятия по защите информации в автоматизированных информационных системах. Законодательство в сфере защиты информации. Государственные и международные стандарты по защите информации. Угрозы безопасности данных и их особенности. Политика защиты информации.

Тема 2. Система информационной безопасности
Каналы проникновения и принципы построения систем защиты. Определение требований к системе защиты информации. Этапы проектирования системы безопасности. Понятие об идентификации пользователя и его особенности. Основные принципы и методы аутентификации. Одноразовые пароли. Сервер аутентификации. Идентификация и аутентификация с

- помощью биометрических данных. Организационные требования. Требования к документированию. Протоколирование, тестирование программ и обработка угроз.
- Тема 3. Программно-технические методы и средства защиты информации
Стратегии защиты: защитная, наступательная, предупреждающая.
Классификация методов и средств защиты информации.
Идентификация терминалов. Электронные замки и блокираторы.
Защита файлов.
- Тема 4. Криптографические механизмы защиты информации в информационных системах
Симметричные криптосистемы. Криптосистемы с открытым ключом. Цифровая подпись. Требования к цифровой подписи.
Правовые аспекты использования цифровой подписи.
Криптосистема шифрования данных RSA. Программный пакет PGP. Криптографическое хеширования.
- Тема 5. Методы криптографического закрытия информации
Шифрование. Классификация основных методов криптографического закрытия информации. Подстановка (замена). Перестановка по методу Гамильтона. Гаммирование.
Аналитические преобразования. Комбинированные методы шифрования.
- Тема 6. Методы кодирования информации
Символьное кодирования. Смысловое кодирование Метод "Стопка книг". Метод Савчука. Одноалфавитное и многоалфавитное смысловое кодирование. Метод рассечения-разнесения данных: механическое и смысловое.
- Тема 7. Методы сжатия-расширения информации
Метод Хаффмана (Дерево Хаффмана). Арифметический код. Zip-модификация алгоритма Лемпеля-Зива. LZW-модификация алгоритма Лемпеля-Зива
- Тема 8. Модели управления доступом
Матричный и мандатный подходы к организации разграничения прав доступа к информации. Права доступа в Windows и Linux.
Пример индивидуальной разработки системы управления доступом.
- Тема 9. Методы хранения данных
RAID массивы. Сохранение данных на скрытых разделах.
Шифрование скрытого раздела жесткого диска. Резервное копирование: инкрементное, дифференциальное, полное.
- Тема 10. Защита программ от изучения
Классификация компьютерных преступлений. Задача защиты от изучения и способы их решения. Вирусы как особый класс разрушающих программных действий. Атаки на сервер. Атаки на рабочие станции. Протоколирование.

4.3. Лекции

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1	Введение в безопасность автоматизированных систем	2	–	0,4
2	Система информационной безопасности	2	–	0,4
3	Программно-технические методы и средства защиты информации	2	–	0,4
4	Криптографические механизмы защиты информации в информационных системах	4	–	0,8
5	Методы криптографического закрытия информации	4	–	0,8
6	Методы кодирования информации	4	–	0,8
7	Методы сжатия-расширения информации	4	–	0,8
8	Модели управления доступом	2	–	0,8
9	Методы хранения данных	2	–	0,4
10	Защита программ от изучения	2	–	0,4
Итого:		28	–	6

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	Практическая работа №1 Аналитические преобразования	2	–	0,5
2.	Практическая работа №2 Кодирование символьное метод "стопка книг"	2	–	0,2
3.	Практическая работа №3 Кодирование символьное метод Савчука	2	–	0,2
4.	Практическая работа №4 Метод рассечения-разнесения данных	2	–	0,1
5.	Практическая работа №5 Арифметический код	2	–	0,5
6.	Практическая работа №6 Построение RAID массивов	2	–	0,3
7.	Практическая работа №7 Организация систем резервного копирования	2	–	0,2
Итого		14	–	2

4.5. Лабораторные работы

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1	Лабораторная работа №1 Криптосистема шифрования данных RSA	6	–	1
2	Лабораторная работа №2 Шифрование перестановкой – гиперкуб Гамильтона	4	–	1
3	Лабораторная работа №3 обратимое XOR шифрование текста со случайной гаммой	6	–	1
4	Лабораторная работа №4 Метод Хаффмана (дерево Хаффмана)	4	–	1
5	Лабораторная работа №5 ZIP-модификация алгоритма Лемпеля-Зива. LZW-модификация алгоритма Лемпеля-Зива	4	–	1
6	Лабораторная работа №6 ZIP-алгоритм сжатия изображений	4	–	1
Итого:		28	–	6

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
1	Введение в безопасность автоматизированных систем	изучение лекционных материалов, подготовка к промежуточному контролю	0	–	2
2	Система информационной безопасности		0	–	2
3	Программно-технические методы и средства защиты информации		0	–	6
4	Криптографические механизмы защиты информации в информационных системах		0	–	8
5	Методы криптографического закрытия информации		0	–	8
6	Методы кодирования информации		0	–	8
7	Методы сжатия-расширения информации		0	–	4
8	Модели управления доступом		0	–	4
9	Методы хранения данных		0	–	4
10	Защита программ от изучения		0	–	4
11	Лабораторная работа №1 Криптосистема шифрования данных RSA	подготовка к лабораторным работам, промежуточному контролю, оформление	2	–	2
12	Лабораторная работа №2 Шифрование перестановкой – гиперкуб Гамильтона		2	–	2

13	Лабораторная работа №3 обратимое XOR шифрование текста со случайной гаммой	отчетов по лабораторным работам	3	–	2
14	Лабораторная работа №4 Метод Хаффмана (дерево Хаффмана)		2	–	2
15	Лабораторная работа №5 ZIP-модификация алгоритма Лемпеля-Зива. LZW-модификация алгоритма Лемпеля-Зива		2	–	2
16	Лабораторная работа №6 ZIP-алгоритм сжатия изображений		2	–	2
17	Практическая работа №1 Аналитические преобразования	подготовка к практическим работам, промежуточному контролю, оформление отчетов по практическим работам	1	–	2
18	Практическая работа №2 Кодирование символьное метод "стопка книг"		1	–	2
19	Практическая работа №3 Кодирование символьное метод Савчука		1	–	2
20	Практическая работа №4 Метод рассечения-разнесения данных		1	–	2
21	Практическая работа №5 Арифметический код		1	–	2
22	Практическая работа №6 Построение RAID массивов		1	–	2
23	Практическая работа №7 Организация систем резервного копирования		1	–	2
24	Решение индивидуальных задач согласно варианта.	выполнение индивидуального задания	18	–	18
Итого:			38	–	94

4.7. Курсовые работы/проекты.

Не планируется.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий:

– традиционные объяснительно-иллюстративные технологии, которые обеспечивают доступность учебного материала для большинства студентов, системность, отработанность организационных форм и привычных методов, относительно малые затраты времени;

– технологии проблемного обучения, направленные на развитие познавательной активности, творческой самостоятельности студентов и

предполагающие последовательное и целенаправленное выдвижение перед студентом познавательных задач, разрешение которых позволяет студентам активно усваивать знания (используются поисковые методы; постановка познавательных задач);

- технологии развивающего обучения, позволяющие ориентировать учебный процесс на потенциальные возможности студентов, их реализацию и развитие;

- технологии концентрированного обучения, суть которых состоит в создании максимально близкой к естественным психологическим особенностям человеческого восприятия структуры учебного процесса и которые дают возможность глубокого и системного изучения содержания учебных дисциплин за счет объединения занятий в тематические блоки;

- технологии модульного обучения, дающие возможность обеспечения гибкости процесса обучения, адаптации его к индивидуальным потребностям и особенностям обучающихся (применяются, как правило, при самостоятельном обучении студентов по индивидуальному учебному плану);

- технологии дифференцированного обучения, обеспечивающие возможность создания оптимальных условий для развития интересов и способностей студентов, в том числе и студентов с особыми образовательными потребностями, что позволяет реализовать в культурно-образовательном пространстве университета идею создания равных возможностей для получения образования

- технологии активного (контекстного) обучения, с помощью которых осуществляется моделирование предметного, проблемного и социального содержания будущей профессиональной деятельности студентов (используются активные и интерактивные методы обучения) и т.д.

6. Формы контроля освоения дисциплины

Текущая аттестация студентов производится в дискретные временные интервалы лектором и преподавателем(ями), ведущими лабораторные работы по дисциплине в следующих формах:

- фронтальные и индивидуальные опросы;
- контрольные работы;
- выполнение лабораторных работ;
- защита лабораторных работ;
- защита индивидуальных заданий.

Фонды оценочных средств, включающие типовые задания и методы контроля, позволяющие оценить результаты текущей и промежуточной аттестации обучающихся по данной дисциплине, помещаются в приложении к рабочей программе в соответствии с «Положением о фонде оценочных средств».

Шкала оценивания	Характеристика знания предмета и ответов
зачтено	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач. Успешно выполняющий предусмотренные в программе задания.
не зачтено	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы. Предусмотренные в программе задания выполнены не полностью.

7. Учебно-методическое и программно-информационное обеспечение дисциплины:

а) основная литература:

Бахаров Л.Е., Информационная безопасность и защита информации (разделы криптография и стеганография) : практикум / Л.Е. Бахаров. – М. : МИСиС, 2019. – 59 с. – ISBN 978-5-906953-94-0 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785906953940.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Орлов В.А., Теория чисел в криптографии : учеб. пособие / В.А. Орлов, Н.В. Медведев, Н.А. Шимко, А.Б. Домрачева – М. : Издательство МГТУ им. Н. Э. Баумана, 2011. – 223 с. – ISBN 978-5-7038-3520-3 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785703835203.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Горбунов В.А., Математические методы в теории защиты информации / Горбунов В.А. – М: Издательство Московского государственного горного университета, 2004. – 82 с. – ISBN 5-7418-0339-3 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN5741803393.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Левина А.Б., Моделирование криптосистем : учебное пособие / Левина А.Б. – СПб.: ИЦ Интермедия, 2017. – 144 с. – ISBN 978-5-4383-0136-3 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785438301363.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

б) дополнительная литература:

Торстейнсон П., Криптография и безопасность в технологии .NET / П. Торстейнсон, Г. А. Ганеш ; пер. с англ. – 3-е изд. (эл.). – М. : БИНОМ, 2015. – 482 с. (Программисту.) – ISBN 978-5-9963-2952-6 – Текст : электронный //

ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785996329526.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Алексеев А.П., Сборник лабораторных работ по дисциплине "Информатика", часть 2 : учебное пособие / Алексеев А.П. – М. : СОЛОН-ПРЕСС, 2017. – 256 с. – ISBN 978-5-91359-170-8 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785913591708.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Страуструп Б., Дизайн и эволюция C++ / Страуструп Б. Пер. с англ. – М. : ДМК Пресс, 2006. – 448 с. (Серия "Для программистов") – ISBN 5-94074-005-7 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN5940740057.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Бьерн Страуструп Язык программирования C++. Второе дополненное издание // Бином. – 2006. – 369 с.

Дейтел П., C для программистов с введением в C11 / Дейтел П., Дейтел Х. – М. : ДМК Пресс, 2014. – 544 с. – ISBN 978-5-97060-073-3 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785970600733.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Шелудько В.М., Основы программирования на языке высокого уровня Python : учебное пособие / Шелудько В. М. – Ростов н/Д : Изд-во ЮФУ, 2017. – 146 с. – ISBN 978-5-9275-2649-9 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785927526499.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

Златопольский Д.М., Основы программирования на языке Python : учебник / Златопольский Д. М. – М. : ДМК Пресс, 2017. – 284 с. – ISBN 978-5-97060-552-3 – Текст : электронный // ЭБС "Консультант студента" : [сайт]. – URL : <http://www.studentlibrary.ru/book/ISBN9785970605523.html> (дата обращения: 01.09.2022) – Режим доступа : по подписке.

в) Интернет-ресурсы:

Библиотека on-line URL: <http://citforum.ru/programming/>

Программирование, статьи, документация по C/C++, Форумы по программированию, исходники. URL: <http://www.proger.ru/>

Сайт, посвященный программированию на Visual C++. URL: <http://programmingcpp.narod.ru/>

Министерство образования и науки Российской Федерации – <http://минобрнауки.рф/>

Федеральная служба по надзору в сфере образования и науки – <http://obrnadzor.gov.ru/>

Портал Федеральных государственных образовательных стандартов высшего образования – <http://fgosvo.ru>

Федеральный портал "Российское образование" – <http://www.edu.ru/>

Информационная система "Единое окно доступа к образовательным ресурсам" – <http://window.edu.ru/>

Федеральный центр информационно-образовательных ресурсов – <http://fcior.edu.ru/>

Электронные библиотечные системы и ресурсы

Электронно-библиотечная система "Консультант студента" – <http://www.studentlibrary.ru/cgi-bin/mb4x>

Электронно-библиотечная система "StudMed.ru" – <https://www.studmed.ru>

Информационный ресурс библиотеки образовательной организации

Научная библиотека имени А. Н. Коняева – <http://biblio.dahluniver.ru/>

8. Материально-техническое обеспечение дисциплины

Освоение дисциплины "Безопасность автоматизированных систем" предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Лекционные занятия: комплект электронных презентаций/слайдов; аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук).

Лабораторные работы: лаборатория "Компьютерный класс", оснащенная прикладным программным обеспечением, приведенным ниже.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет, рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Программное обеспечение:

Функциональное назначение	Бесплатное программное обеспечение	Ссылки
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Бесплатное IDE, разрабатывается как программное обеспечение с открытым исходным кодом.	Visual Studio Code	https://code.visualstudio.com/