Учреждение образования
«Полоцкий государственный университет имени Евфросинии Полоцкой»

УТВЕРЖДАЮ
Ректор учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
_____ Ю.Я. Романовский
«15» _____ 2025 г.

Регистрационный № УД–3689/25уч.

БЕЗОПАСНОСТЬ ОБЛАЧНЫХ И ВЕБ ТЕХНОЛОГИЙ

Учебная программа учреждения образования
по учебной дисциплине для специальности
6-05-0533-12 «Кибербезопасность»

2025 г.

Учебная программа составлена на основе образовательного стандарта по специальности высшего образования ОСВО 6-05-0533-12 – 2023 и учебного плана по специальности 6-05-0533-12 «Кибербезопасность». Регистрационный № 14-23/уч. ФКНЭ от 04.04.2023г. для дневной формы получения высшего образования

СОСТАВИТЕЛЬ:
МАТЕЛЕНОК Анастасия Петровна, кандидат педагогических наук, доцент, доцент кафедры математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой математики и компьютерной безопасности учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 11 от «21» 11 2025 г.);

Научно-методическим советом учреждения образования «Полоцкий государственный университет имени Евфросинии Полоцкой»
(протокол № 3 от «15» 12 2025 г.)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Современная информационно-коммуникационная экосистема базируется на двух фундаментальных парадигмах: веб-ориентированной модели распределения сервисов и облачных вычислениях как модели предоставления масштабируемых вычислительных ресурсов. Конвергенция этих парадигм привела к формированию гибридных архитектур, где границы периметра безопасности становятся размытыми и динамичными. В этих условиях изучение дисциплины «Безопасность облачных и веб технологий» позволяет понимать особенности этих сервисов. Они предоставляют возможность хранить данные на удаленных серверах через интернет. Это дает возможность сэкономить место на ПК и получать доступ к интересующим файлам из любого удобного места.

Цель учебной дисциплины – сформировать у обучающихся системное теоретическое знание и практические компетенции в области проектирования, реализации и обеспечения безопасности распределенных информационных систем, построенных на основе веб-технологий и парадигмы облачных вычислений, в соответствии с современными архитектурными принципами и нормативными требованиями.

Задачи учебной дисциплины:

• выработать навыки анализа защищенности (Security Assessment): проведение ревью кода на предмет типовых уязвимостей, аудит конфигураций облачных сервисов (AWS, Azure, GCP), использование инструментов статического и динамического анализа (SAST/DAST);

• приобрести опыт построения облачных архитектур в том числе для прикладных областей с большой долей математического моделирования;

• научить проводить оценку рисков (Risk Assessment) для облачных проектов, выбирать адекватные средства контроля (security controls) и обосновывать экономическую целесообразность мер защиты;

• сформировать системное (архитектурное) мышление, позволяющее видеть взаимосвязь между бизнес-требованиями, технологическим стеком и мерами безопасности в условиях распределенной, динамически изменяющейся IT-среды.

В результате изучения учебной дисциплины «Безопасность облачных и веб технологий» формируются следующие **специализированные компетенции:**

- Разрабатывать программное обеспечение в интегрированных средах разработки. Использовать автоматизированные средства разработки программных средств. Разрабатывать необходимую для этого документацию.

- Владеть базовыми принципами построения компьютерных систем и сетей, алгоритмами маршрутизации в IP-сетях, создавать сетевые приложения, использующие базовые протоколы.

В результате изучения учебной дисциплины магистрант должен:

знать:

- актуальные тактики, техники и процедуры (TTP), используемые злоумышленниками против веб-приложений и облачных сред;
- ключевые риски облачных вычислений по Cloud Security Alliance (CSA);
- принципы и компоненты архитектуры нулевого доверия;
- особенности безопасности микросервисных архитектур, контейнеров (Docker) и оркестраторов (Kubernetes);
- модели жизненного цикла разработки безопасного ПО;
- методы безопасного хранения аутентификационных данных (хэширование, соление, адаптивные функции);
- основы управления криптографическими ключами;
- национальные требования в сфере защиты персональных данных и требования регуляторов к облачным сервисам,

уметь:

- проводить ручной аудит веб-приложения на наличие распространенных уязвимостей (инъекции, XSS, небезопасные десериализации);
- анализировать конфигурации облачных сервисов (S3, IAM, Security Groups/NSG) на соответствие best practices;
- читать и интерпретировать результаты автоматизированного сканирования (отчеты SAST/DAST, облачные security scores);
- оценивать риски безопасности для предлагаемой облачной архитектуры;
- настраивать мониторинг и логирование (CloudTrail, Activity Log, SIEM-интеграции) для ключевых событий безопасности;
- реализовывать безопасные практики для контейнеров (сканирование образов, запуск с минимальными привилегиями);
- проектировать и развертывать информационные сервисы в облаке;
- анализировать риски и архитектуру информационных систем в облаке,

владеть:

- навыками работы с инструментами для пентеста веб-приложений;
- навыками аудита облачных конфигураций с помощью встроенных средств (AWS Security Hub, Azure Security Center, GCP Security Command Center) или инструментов типа Prowler, ScoutSuite;
- базовыми навыками анализа сетевого трафика и логов (Wireshark, анализ журналов веб-сервера, CloudTrail);
- навыками написания простых скриптов (на Python, Bash, PowerShell) для автоматизации рутинных проверок безопасности;

- навыками следования методологии безопасной разработки (Secure Coding Guidelines);
- навыками документирования процедур и политик безопасности (например, политики использования облачных сервисов);
- навыками презентации результатов аудита и обоснования необходимых контрмер техническим и нетехническим стейкхолдерам.

Связи с другими учебными дисциплинами

Базовыми учебными дисциплинами для учебной дисциплины «Безопасность облачных и веб технологий» являются «Архитектура компьютеров», «Компьютерные сети», «Основы кибербезопасности», «Криптографические методы защиты информации», «Защита от вредоносного программного обеспечения» и «Надежность программного обеспечения». В свою очередь учебная дисциплина «Безопасность облачных и веб технологий» является базой для специальных учебных дисциплин, например, «Технологии разработки и защиты веб-приложений и веб-служб», «Методы и стандарты оценки защищенности компьютерных систем» и «Безопасность информационных систем».

Форма получения высшего образования – дневная.

В соответствии с учебным планом специальности 6-05-0533-12 «Кибербезопасность», учебная программа предусматривает для изучения дисциплины следующее распределение учебных часов:

Курс	3
Семестр	6
Лекции (количество часов)	32
Практические занятия (количество часов)	18
Аудиторных часов по учебной дисциплине	50
Самостоятельная работа (количество часов)	58
Всего часов по учебной дисциплине	108
Трудоемкость учебной дисциплины, з.е.	3
Форма промежуточной аттестации	зачет

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

1. Введение. История и развития облачных и веб-технологий. Практика. Регистрация на популярных облачных платформах.
2. Модели предоставления облачных сервисов. Iaas,PaaS, Saas. Определения и различия. Преимущества и недостатки каждой модели.
3. Архетиктура и компоненты облачных решений. Основные элементы облачной архитектуры.
4. Виртуализация и управление ресурсами. Создание виртуальной машины.
5. Безопасность в облачных технологиях. Основные угрозы и меры защиты. Управление доступом и индентификация. Настройка прав доступа и политик безопасности.
6. Хранение данных в облаке. Особенности облачных хранилищ. Резервное копирование и восстановление данных. Работа с облачным хранилищем.
7. Облачные решения для бизнеса и повседневной жизни. Применение SaaS-решений в бизнесе. Облачные сервисы для личного использования. Работа с облачными приложениями для командной работы.
8. Оптимизация затрат при использовании облака. Модели ценообразования в облачных сервисах. Мониторинг и анализ расходов на облачные сервисы.
9. Миграция на облачные платформы. Подготовка и планирование миграции. Перенос данных и приложений в облако. Миграция небольшого проекта в облако.
10. Интеграция облачных решений. Совмещение облачных и локальных ресурсов. API инструменты интеграции. Интеграция облачного сервиса с локальным приложением.
11. Построение и управление облачной инфраструктурой. Основы управления облачными ресурсами. Автоматизация и оркестрация в облаке. Настройка и автоматизация облачной инфраструктуры.
12. Веб-приложения. Структура современных веб-приложений. Поиск субдоменов. Анализ API. Обнаружение сторонних зависимостей. Поиск слабых мест в архитектуре приложения.

13. Взлом веб-приложений. Межсайтовый скриптинг. Подделка межсайтовых запросов Атака на внешние сущности XML. Внедрение кода. Отказ в обслуживании.

14. Защита современных веб-приложений. Безопасная архитектура приложений. Проверка безопасности кода. Обнаружение уязвимостей. Управление уязвимостями.

15. Противодействие XSS-атакам. Защита от CSRF. Защита от XXE-атак. Противодействие внедрению.

16. Противодействие DoS-атакам. Защита сторонних зависимостей.

Учебно-методическая карта учебной дисциплины
«БЕЗОПАСНОСТЬ ОБЛАЧНЫХ И ВЕБ ТЕХНОЛОГИЙ»

Дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов		Форма контроля знаний	Литература
		Лекции	Практические занятия		
1	2	3	4	6	
	6 СЕМЕСТР				
1.	Введение. История и развития облачных и веб-технологий. Практика. Регистрация на популярных облачных платформах.	2			[5]
2.	Модели предоставления облачных сервисов. Iaas,PaaS, Saas. Определения и различия. Преимущества и недостатки каждой модели.	2			[5]
3.	Архетиктура и компоненты облачных решений. Основные элементы облачной архитектуры.	2	2	ИЗ, ОПР*	[5]
4.	Виртуализация и управление ресурсами. Создание виртуальной машины.	2	2	ИЗ, ОПР*	[1,2]
5.	Безопасность в облачных технологиях. Основные угрозы и меры защиты. Управление доступом и индентификация. Настройка прав доступа и политик безопасности.	2	2	ИЗ, ОПР*	[1,2]
6.	Хранение данных в облаке. Особенности облачных хранилищ. Резервное копирование и восстановление данных. Работа с облачным хранилищем.	2			[1,2]
7.	Облачные решения для бизнеса и повседневной жизни. Применение SaaS-решений в бизнесе. Облачные сервисы для личного использования. Работа с облачными приложениями для командной работы.	2	2	ИЗ, ОПР*	[1,2]
8.	Оптимизация затрат при использовании облака. Модели ценообразования в облачных сервисах. Мониторинг и анализ расходов на облачные сервисы.	2	2	ИЗ, ОПР*	[1,2]
9.	Миграция на облачные платформы. Подготовка и планирование миграции. Перенос данных и приложений в облако. Миграция небольшого проекта в облако.	2	2	ИЗ, ОПР*	[1,2]
10.	Интеграция облачных решений. Совмещение облачных и локальных ресурсов. API инструменты интеграции. Интеграция облачного сервиса с локальным приложением.	2			[1,2]
11.	Построение и управление облачной инфраструктурой. Основы управления облачными ресурсами. Автоматизация и оркестрация в облаке. Настройка и автоматизация облачной инфраструктуры.	2			[1,2]

12.	Веб-приложения. Структура современных веб-приложений. Поиск субдоменов. Анализ API. Обнаружение сторонних зависимостей. Поиск слабых мест в архитектуре приложения.	2			[1,2]
13.	Взлом веб-приложений. Межсайтовый скриптинг. Подделка межсайтовых запросов Атака на внешние сущности XML. Внедрение кода. Отказ в обслуживании.	2	2	ИЗ, ОПР*	[1,2]
14.	Защита современных веб-приложений. Безопасная архитектура приложений. Проверка безопасности кода. Обнаружение уязвимостей. Управление уязвимостями.	2	2	КР* ИЗ, ОПР*	[1,2]
15.	Противодействие XSS-атакам. Защита от CSRF. Защита от XXE-атак. Противодействие внедрению.	2	2	ИЗ, ОПР*	[1,2]
16.	Противодействие DoS-атакам. Защита сторонних зависимостей.	2			[1,2]
	Всего	**32**	**18**		

* мероприятия текущего контроля

Принятые сокращения:

ИЗ – индивидуальное задание;
ОПР – отчет о выполнении практической работы;
КР – контрольная работа.

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

ЛИТЕРАТУРА

Основная:

1. Гифт, Н. Прагматичный ИИ: машинное обучение и облачные технологии = Pragmatic AI: an introduction to cloud-based machine learning / пер. с англ. И. Пальти. - Санкт-Петербург : Питер, 2019. - 300 с. : ил. - (Для профессионалов).

2. Ибрам, Б. Паттерны Kubernetes : шаблоны разработки собственных облачных приложений = Kubernetes Patterns : Reusable Elements for Designing Cloud-Native Applications / пер. с англ. А. Киселев. - Санкт-Петербург : Питер, 2020. - 316 с.

3. Облачные архитектуры : разработка устойчивых и экономичных облачных приложений = Cloud native architectures / Том Лащевски, Камаль Арора, Эрик Фарр, Пийюм Зонуз; перевел с английского А. Павлов. - Санкт-Петербург : Питер, 2022. - 320 с.

4. Хоффман, Э. Безопасность веб-приложений : разведка, защита, нападение / [перевела с английского И. Рузмайкина]. - Санкт-Петербург : Питер, 2024. - 327, [1] с. : ил. - (Бестселлеры O'Reilly).

5. Таненбаум, Э. Современные операционные системы = Modern operating systems / пер. с англ. А. Леонтьева, М. Малышева, Н. Вильчинский. - . - Санкт-Петербург : Питер, 2024. - 1119 с. : ил., табл. - (Классика computer science).

Дополнительная:

6. Безопасность операционных систем: учебное пособие / под редакцией С.В. Скрыля. - Москва : Издательский центр "Академия", 2021. - 254 с. - (Бакалавриат; Высшее образование). - Рекомендовано Федеральным учебно-методическим объединением в системе высшего образования по укрупненной группе специальностей и направлений подготовки "Информационная безопасность" в качестве учебного пособия для студентов, обучающихся по специальностям "Компьютерная безопасность" и "Информационная безопасность автоматизированных систем" и направлению подготовки "Информационная безопасность"-бакалавриат

7. Чакон, С. Git для профессионального программиста = Pro Git / пер. с англ. И. Рузмайкина. - Санкт-Петербург : Питер, 2022. - 494 с. : ил. - (Библиотека программиста).

Гудкова Е.В.

ХАРАКТЕРИСТИКА ИННОВАЦИОННЫХ ПОДХОДОВ К ПРЕПОДАВАНИЮ УЧЕБНОЙ ДИСЦИПЛИНЫ

В преподавании дисциплины используются:

–методы проблемного обучения (проблемное изложение, частично-поисковый и исследовательский методы);

–личностно ориентированные (развивающие) технологии, основанные на активных (рефлексивно-деятельностных) формах и методах обучения («мозговой штурм», дискуссия, пресс-конференция);

- информационно-коммуникационные технологии, обеспечивающие проблемно-исследовательский характер процесса обучения и активизацию самостоятельной работы студентов (структурированные электронные презентации для лекционных занятий, использование аудио-, видеоподдержки учебных занятий, примененение специализированных компьютерных программ.

ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПРОВЕДЕНИЯ ЗАЧЕТА

1. История и развития облачных и веб-технологий.
2. Регистрация на популярных облачных платформах.
3. Модели предоставления облачных сервисов. Iaas,PaaS, Saas. Определения и различия. Преимущества и недостатки каждой модели.
4. Архетиктура и компоненты облачных решений.
5. Основные элементы облачной архитектуры. Виртуализация и управление ресурсами.
6. Создание виртуальной машины. Безопасность в облачных технологиях. Основные угрозы и меры защиты.
7. Управление доступом и индентификация. Настройка прав доступа и политик безопасности.
8. Хранение данных в облаке. Особенности облачных хранилищ.
9. Резервное копирование и восстановление данных. Работа с облачным хранилищем. Облачные решения для бизнеса и повседневной жизни.
10. Применение SaaS-решений в бизнесе. Облачные сервисы для личного использования.
11. Работа с облачными приложениями для командной работы.
12. Оптимизация затрат при использовании облака. Модели ценообразования в облачных сервисах. Мониторинг и анализ расходов на облачные сервисы.
13. Миграция на облачные платформы. Подготовка и планирование миграции. Перенос данных и приложений в облако. Миграция небольшого проекта в облако
14. Интеграция облачных решений. Совмещение облачных и локальных ресурсов. API инструменты интеграции. Интеграция облачного сервиса с локальным приложением.
15. Построение и управление облачной инфраструктурой. Основы управления облачными ресурсами.
16. Автоматизация и оркестрация в облаке. Настройка и автоматизация облачной инфраструктуры.
17. Веб-приложения. Структура современных веб-приложений. Поиск субдоменов. Анализ API. Обнаружение сторонних зависимостей.
18. Поиск слабых мест в архитектуре приложения. Взлом веб-приложений.
19. Межсайтовый скриптинг. Подделка межсайтовых запросов Атака на внешние сущности XML. Внедрение кода. Отказ в обслуживании.

20. Защита современных веб-приложений. Безопасная архитектура приложений. Проверка безопасности кода.
21. Обнаружение уязвимостей. Управление уязвимостями. Противодействие XSS-атакам. Защита от CSRF.
22. Защита от XXE-атак. Противодействие внедрению.
23. Противодействие DoS-атакам. Защита сторонних зависимостей.

ОРГАНИЗАЦИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

Цель самостоятельной работы студентов – содействие усвоению в полном объеме содержания учебной дисциплины и формирование самостоятельности как личностной черты и важного профессионального качества, сущность которых состоит в умении систематизации, планирования и контроля собственной деятельности. Задача самостоятельной работы студентов – усвоение определенных стандартом знаний, умений и навыков по учебной дисциплине, закрепление и систематизация полученных знаний, их применение при выполнении практических работ и творческих работ, а также выявление пробелов в системе знаний по учебной дисциплине.

При изучении дисциплины используются следующие формы самостоятельной работы:

–подготовка к контрольным работам;

- подготовка к выполнениюпрактических работ, с консультациями преподавателя и подготовка отчета для их защиты.

Методы планирования и организации самостоятельной работы студентов

- анализ учебной программы по учебной дисциплине «Безопасность облачных и веб технологий» с целью выделения тематических блоков для самостоятельной работы студентов;
- проработка баланса времени, необходимого для самостоятельной работы студентов с выделенными тематическими блоками;
- структурирование тематических заданий, ориентированных на формирование и развитие компетенций студентов в контексте самостоятельной работы.

Содержание самостоятельной работы студентов дневной формы получения высшего образования

	Тематическое содержание	Используемые источники	К-во часов (58 ч)
			6 семестр
Углубленное изучение теоретической части	Введение. История и развития облачных и веб-технологий. Практика. Регистрация на популярных облачных платформах.	[1],[2],[3],[8]	4
	Модели предоставления облачных сервисов. Iaas,PaaS, Saas. Определения и различия. Преимущества и недостатки каждой модели.	[1],[2],[3],[8]	4
	Архетиктура и компоненты облачных решений. Основные элементы облачной архитектуры.	[1],[2],[3],[8]	4
	Виртуализация и управление ресурсами. Создание виртуальной машины.	[1],[2],[3]	4
	Безопасность в облачных технологиях. Основные угрозы и меры защиты. Управление доступом и индентификация. Настройка прав доступа и политик безопасности.	[1],[2],[3],[7]	4
	Хранение данных в облаке. Особенности облачных хранилищ. Резервное копирование и восстановление данных. Работа с облачным хранилищем.	1[1],[2],[7],[8]	4
	Облачные решения для бизнеса и повседневной жизни. Применение SaaS-решений в бизнесе. Облачные сервисы для личного использования. Работа с облачными приложениями для командной работы.	[1],[2],[3]	4
	Оптимизация затрат при использовании облака. Модели ценообразования в облачных сервисах. Мониторинг и анализ расходов на облачные сервисы.	[1],[2],[3]	4
	Миграция на облачные платформы. Подготовка и планирование миграции. Перенос данных и приложений в облако. Миграция небольшого проекта в облако.	[1],[2],[3],[6]	2
	Интеграция облачных решений. Совмещение облачных и локальных ресурсов. API инструменты интеграции. Интеграция облачного сервиса с локальным приложением.	[1],[2],[3],[6]	2
	Построение и управление облачной инфраструктурой. Основы управления облачными ресурсами. Автоматизация и оркестрация в облаке. Настройка и автоматизация облачной инфраструктуры.	[1],[2],[3],[6]	2
	Веб-приложения. Структура современных веб-приложений. Поиск субдоменов. Анализ API. Обнаружение сторонних зависимостей. Поиск слабых мест в архитектуре приложения.	[1],[2],[3],[6]	2

	Взлом веб-приложений. Межсайтовый скриптинг. Подделка межсайтовых запросов Атака на внешние сущности XML. Внедрение кода. Отказ в обслуживании.	[1],[2],[3],[6]	2
	Защита современных веб-приложений. Безопасная архитектура приложений. Проверка безопасности кода. Обнаружение уязвимостей. Управление уязвимостями.	[1],[2],[3],[6]	4
	Противодействие XSS-атакам. Защита от CSRF. Защита от XXE-атак. Противодействие внедрению.	[1],[2],[3],[6]	4
	Противодействие DoS-атакам. Защита сторонних зависимостей.	[1],[2],[3],[6]	4
	Подготовка к контрольной работе	[1],[2],[3],[6]	4
	ВСЕГО		58

КОНТРОЛЬ КАЧЕСТВА УСВОЕНИЯ ЗНАНИЙ

6 семестр

Диагностика качества усвоение знаний проводится в форме текущего контроля и промежуточной аттестации.

Средства диагностики результатов учебной деятельности:

Для оценки достижений студентов используется следующий диагностический инструментарий:

- письменный отчет по практической работе;
- контрольная работа;
- зачет.

Результат текущего контроля за семестр оценивается отметкой в баллах по десятибалльной шкале и выводится исходя из отметок, выставленных в ходе проведения мероприятий текущего контроля в течении семестра по следующей формуле:

$$Т = ТК_1 + ТК_2 + \ldots..ТК_n / n,$$

где Т – отметка за семестр по результатам текущего контроля; в случае, если Т – дробное число, оно округляется по правилам математического округления;

ТК– отметки, выставленная за письменные отчеты по практическим работам и за контрольную работу.

n – мероприятий текущего контроля;

Текущие контрольные мероприятия	*Рейтинговая контрольная работа*
Содержание контрольного мероприятия – название раздела (модуля)	Защита современных веб-приложений. Безопасная архитектура приложений. Проверка безопасности кода. Обнаружение уязвимостей. Управление уязвимостями.
Задания	Контрольное задание состоит из 2 задач
Отметка контрольных мероприятий	Каждый пункт оценивается в 5 балла

Промежуточная аттестация проводится в форме зачета.

Если отметка за семестр $T \geq 4$, то студент получает отметку «зачтено».

Если отметка за семестр $T < 4$, то студент получает отметку «не зачтено» и ему следует переписать контрольную работу и до сдать отчет по практической работе.

ПЕРЕЧЕНЬ КОМПЬЮТЕРНЫХ ПРОГРАММ

Microsoft Office Excel ver. 2003 и выше, MATHCAD 2000 PROFESSIONAL и выше, MAPLE 12 и выше, MATLAB 5 и выше, SPSS.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ С ДРУГИМИ УЧЕБНЫМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу
Технологии разработки и защиты веб-приложений и веб-служб	кафедра математики и компьютерной безопасности	нет	
Методы и стандарты оценки защищенности компьютерных систем	кафедра математики и компьютерной безопасности	нет	
Безопасность информационных систем	кафедра математики и компьютерной безопасности	нет	

Заведующий кафедрой математики и
компьютерной безопасности,
к.т.н., доцент И.Б. Бураченок