Автономная некоммерческая организация профессионального образования
«Колледж мировой экономики и передовых технологий»

РАБОЧАЯ ПРОГРАММА

учебной дисциплины ОП.14. Информационная безопасность

по специальности
09.02.07 Информационные системы и программирование

форма обучения – очная
квалификация – программист

Москва – 2021

РАССМОТРЕНА

на заседании Педагогического совета
Протокол от 30 августа 2021г. № 1

Разработана на основе Федерального государственного образовательного стандарта по специальности среднего профессионального образования
09.02.07 Информационные системы и программирование

Заместитель директора по методической работе

_____ / Ю. И. Богомолова
Подпись ФИО

Организация-разработчик:

АНО ПО «Колледж мировой экономики и передовых технологий»

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ ОП.14. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью образовательной программы в соответствии с ФГОС по специальности СПО 09.02.07 Информационные системы и программирование.

1.2. Место дисциплины в структуре образовательной программы:

Учебная дисциплина ОП.14. Информационная безопасность принадлежит к общепрофессиональному циклу.

В результате освоения образовательной программы у выпускника должны быть сформированы общие и профессиональные компетенции.

Выпускник, освоивший образовательную программу, должен обладать следующими общими компетенциями (далее – ОК):

ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности

ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.

ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.

ОК 09. Использовать информационные технологии в профессиональной деятельности

ОК.10 Пользоваться профессиональной документацией на государственном и иностранном языках.

Выпускник, освоивший образовательную программу, должен обладать профессиональными компетенциями (далее - ПК), соответствующими основным видам деятельности:

ПК 1.4. Обеспечивать защиту программного обеспечения компьютерных систем программными средствами.

ПК 4.5. Администрировать базы данных.

ПК 4.6. Защищать информацию в базе данных с использованием технологии защиты информации.

1.3. Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Цель изучения дисциплины – защита национальных интересов; обеспечение человека и общества достоверной и полной информацией; правовая защита человека и общества при получении, распространении и использовании информации.

Задачами являются: анализ производительности и надежности, управление безопасностью, учет трафика, управление конфигурацией.

В результате освоения дисциплины студент *должен знать:*

– основные средства и методы защиты компьютерных систем программными и аппаратными средствами;
– технологии передачи и обмена данными в компьютерных сетях;
– алгоритм проведения процедуры резервного копирования;
– алгоритм проведения процедуры восстановления базы данных;
– методы организации целостности данных;
– способы контроля доступа к данным и управления привилегиями;
– основы разработки приложений баз данных;
– основные методы и средства защиты данных в базе данных.

В результате освоения дисциплины студент *должен уметь:*

– использовать методы защиты программного обеспечения компьютерных систем;
– анализировать риски и характеристики качества программного обеспечения;
– выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами;
– применять стандартные методы для защиты объектов базы данных;
– выполнять стандартные процедуры резервного копирования и мониторинга выполнения этой процедуры;
– выполнять процедуру восстановления базы данных и вести мониторинг выполнения этой процедуры;
– выполнять установку и настройку программного обеспечения для обеспечения работы пользователя с базой данных;
– обеспечивать информационную безопасность на уровне базы данных.

1.4. Количество часов на освоение программы дисциплины:

Объем образовательной программы – **46** часов, в том числе:
занятия во взаимодействии с преподавателем – 36 часов;
самостоятельной работы обучающегося – 10 часов.
Форма итоговой аттестации: дифференцированный зачет.

При угрозе возникновения и (или) возникновении отдельных чрезвычайных ситуаций, введении режима повышенной готовности или чрезвычайной ситуации на всей территории Российской Федерации либо на ее части реализация рабочей программы учебной дисциплины может осуществляться с применением электронного обучения, дистанционных образовательных технологий.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Объем образовательной программы	**46**
Занятия во взаимодействии с преподавателем	**34**
в том числе:	
теоретические занятия	14
лабораторные занятия *(не предусмотрены)*	-
практические занятия	20
контрольные работы *(не предусмотрены)*	-
курсовая работа (проект) *(не предусмотрен)*	-
Самостоятельная работа обучающегося (всего)	**10**
в том числе:	
самостоятельная работа над курсовой работой (проектом) *(не предусмотрено)*	-
Итоговая аттестация в форме дифференцированного зачета	**2**

2.2. Тематический план и содержание учебной дисциплины
ОП.14. Информационная безопасность

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся, курсовая работ (проект) *(если предусмотрены)*		Объем в часах	Коды компетенций, формированию которых способствует элемент программы	Уровень освоения
1	**2**		**3**	***4***	***5***
Раздел 1. Борьба с угрозами несанкционированного доступа к информации					
Тема 1.1. Актуальность проблемы обеспечения безопасности информации Безопасность БД, угрозы, защита	**Содержание учебного материала**		**2**		
	1	Основные понятия безопасности: конфиденциальность, целостность, доступность. Объекты, цели и задачи защиты информации. Возможные угрозы информационной безопасности: классификация, источники возникновения и пути реализации. Виды угроз. Определение требований к уровню обеспечения информационной безопасности. Управление рисками. Основные понятия. Процесс оценки рисков. Понятие безопасности БД. Угрозы безопасности БД: общие и специфичные. Требования безопасности БД. История развития, назначение и роль баз данных. Модели данных. Математические основы построения реляционных СУБД	2	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10 ПК 1.4 ПК 4.5 ПК 4.6	1
	Лабораторные работы *(не предусмотрены)*		-		
	Практические занятия		**4**		
	1	Обзор нормативных правовых актов, нормативных методических документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов	2		2
	2	Анализ рисков информационной безопасности	2		2

	Контрольные работы *(не предусмотрены)*		-		
	Внеаудиторная самостоятельная работа обучающихся		**2**		
	1	Доклад на тему: «Защита информации, тайна»	2		3
Тема 1.2. Критерии защищенности БД	**Содержание учебного материала**		**1**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	1	Критерии оценки надежных компьютерных систем (TCSEC). Понятие политики безопасности. Совместное применение различных политик безопасности в рамках единой модели. Интерпретация TCSEC для надежных СУБД (TDI). Оценка надежности СУБД как компоненты вычислительной системы.	1		1
	Лабораторные работы *(не предусмотрены)*		-		
	Практическое занятие *(не предусмотрены)*		-		
	Контрольные работы *(не предусмотрены)*		-		
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-		
Тема 1.3. Модели безопасности в СУБД	**Содержание учебного материала**		**1**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	1	Дискреционная (избирательная) и мандатная (полномочная) модели безопасности. Классификация моделей. Аспекты исследования моделей безопасности. Особенности применения моделей безопасности в СУБД.	1		1
	Лабораторные работы *(не предусмотрены)*		-		
	Практическое занятие		**2**		
	3	Изучение механизмов защиты СУБД MS ACCESS	2		2
	Контрольные работы *(не предусмотрены)*				
	Внеаудиторная самостоятельная работа обучающихся		**2**		
	2	Подготовка сообщения на тему: «Схема идентификации Гиллоу - Куискуотера.»	2		3
Тема 1.4. Средства идентификации и аутентификации	**Содержание учебного материала**		**1**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4.	
	1	Общие сведения. Совместное применение средств идентификации и аутентификации, встроенных в СУБД и в ОС.	1		1
	Лабораторные работы *(не предусмотрены)*		-		
	Практическое занятие		**2**		
	4	Идентификация и аутентификация объектов сети.	2		2
	Контрольные работы *(не предусмотрены)*		-		
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-		

			ПК 4.5. ПК 4.6.	
Тема 1.5. Средства управления доступом	**Содержание учебного материала**	**1**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	1 Основные понятия: субъекты и объекты, группы пользователей, привилегии, роли и представления. Виды привилегий: привилегии безопасности и доступа. Использование ролей и привилегий пользователей. Соотношение прав доступа, определяемых ОС и СУБД. Использование представлений для обеспечения конфиденциальности информации в СУБД. Средства реализации мандатной политики безопасности в СУБД.	1		1
	Лабораторные работы *(не предусмотрены)*	-		
	Практическое занятие	**2**		
	5 Использование ролей и привилегий пользователей.	2		2
	Контрольные работы *(не предусмотрены)*	-		
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*	-		
Тема 1.6. Целостность БД и способы ее обеспечения	**Содержание учебного материала**	**1**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	1 Основные виды и причины возникновения угроз целостности. Способы противодействия. Цели использования триггеров. Способы задания, моменты выполнения. Декларативная и процедурная ссылочные целостности. Внешний ключ. Способы поддержания ссылочной целостности.	1		1
	Лабораторные работы *(не предусмотрены)*	-		
	Практические занятия *(не предусмотрены)*	-		
	Контрольные работы *(не предусмотрены)*	-		
	Внеаудиторная самостоятельная работа обучающихся	**2**		3
	3 Сообщение/презентация на тему: «Три вида возможных нарушений информационной системы.»	2		2
Тема 1.7. Классификация угроз конфиденциальност и СУБД	**Содержание учебного материала**	**1**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09.	
	1 причины, виды, основные методы нарушения конфиденциальности. Типы утечки конфиденциальной информации из СУБД, частичное разглашение. Получение несанкционированного доступа к конфиденциальной информации путем логических выводов. Методы	1		1

		противодействия. Особенности применения криптографических методов.		ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	Лабораторные работы *(не предусмотрены)*		-		
	Практическое занятие		**2**		
	6	Получение несанкционированного доступа к конфиденциальной информации путем логических выводов.	2		2
	Контрольные работы *(не предусмотрены)*		-		
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-		
Тема 1.8. Аудит и подотчетность	**Содержание учебного материала**		**2**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	1	Подотчетность действий пользователя и аудит связанных с безопасностью событий. Регистрация действий пользователя. Управление набором регистрируемых событий. Анализ регистрационной информации.	2		1
	Лабораторные работы *(не предусмотрены)*				
	Практическое занятие.		**4**		
	7	Регистрация событий (аудит).	2		2
	8	Настройка параметров регистрации и аудита операционной системы	2		2
	Контрольные работы *(не предусмотрены)*		-		
	Внеаудиторная самостоятельная работа обучающихся *(не предусмотрены)*		-		
Тема 1.9. Транзакции и блокировки	**Содержание учебного материала**		**2**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	1	Транзакции как средство изолированности пользователей. Сериализация транзакций. Методы сериализации транзакций. Режимы блокировок. Правила согласования блокировок. Двухфазный протокол синхронизационных блокировок. Тупиковые ситуации, их распознавание и разрушение.	2		1
	Лабораторные работы *(не предусмотрены)*		-		
	Практическое занятие		**2**		
	9	Применение транзакций как средства изолированности пользователей. Режимы блокировок.	2		1
	Контрольные работы *(не предусмотрены)*		-		
	Внеаудиторная самостоятельная работа обучающихся		**2**		
	4	Написание сообщения на тему: «Целостность кода приложения. SQL-	2		3

		инъекции. Динамическое выполнение кода SQL и PL/SQL. Категории атак SQL-инъекцией. Методы SQL-инъекций».			
Тема 1.10. Стандартные методы защиты объектов базы данных	**Содержание учебного материала**		**2**	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	
	1	Основные понятия и определения. Понятие криптографического протокола. Методы аутентификации, использующие пароли и PIN-коды: на основе многоразовых паролей, на основе одноразовых паролей, на основе сертификатов. Строгая аутентификация, основанная: на симметричных алгоритмах, на асимметричных алгоритмах, на однонаправленных хеш-функциях. Биометрическая аутентификация пользователя.	2		1
	Лабораторные работы *(не предусмотрены)*		-		
	Практическое занятие		**2**		
	10	Методы криптографии	2		2
	Контрольные работы *(не предусмотрены)*		-		
	Внеаудиторная самостоятельная работа обучающихся		**2**		
	5	Сообщение/презентация по теме «Криптоанализ», «Электронно-цифровая подпись»	2		3
Дифференцированный зачет			**2**		3
Всего:			**46**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. – ознакомительный (узнавание ранее изученных объектов, свойств);
2. – репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3. – продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Лаборатория программирования и баз данных.

Оборудование лаборатории:

1. комплекты специализированной учебной мебели,
2. маркерная доска,

Технические средства обучения:

1. проектор,
2. экран,
3. автоматизированные рабочие места по количеству обучающихся (не менее 12-15 АРМ) (Core i5, оперативная память объемом 8GB, монитор 23.8", мышь, клавиатура) с выходом в сеть «Интернет» и доступом в электронную информационно-образовательную среду, , МФУ формата А4.
4. Лицензионное программное обеспечение общего и профессионального назначения, в т.ч. ОС Windows, MS Office, 7-Zip , Adobe Acrobat Reader, Comodo Internet Security, Bloodshed Dev-C++, Apache NetBeans, MySQL for Windows, Android Studio
5. Доступы с компьютеров каб. 405 к серверу в каб. 110 (8-х ядерный процессор с частотой 3 ГГц, оперативная память объемом 16 Гб, жесткие диски общим объемом не менее 1 Тб, программное обеспечение: WindowsServer).

3.2. Информационное обеспечение обучения

Перечень учебных изданий, дополнительной литературы, Интернет-источников

Основные источники:

1. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. – Москва: Издательство Юрайт, 2021. – 342 с. – (Профессиональное образование). – ISBN 978-5-534-10671-8. – URL: https://urait.ru/bcode/475889

Дополнительные источники:

1. Внуков, А. А. Основы информационной безопасности: защита информации: учебное пособие для среднего профессионального образования / А. А. Внуков. – 3-е изд., перераб. и доп. – Москва: Издательство Юрайт, 2021. – 161 с. – (Профессиональное образование). – ISBN 978-5-534-13948-8. – URL: https://urait.ru/bcode/475890

2. Суворова. Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. – Москва: Издательство Юрайт, 2021. – 253 с. – (Высшее образование). – ISBN 978-5-534-13960-0. – URL: https://urait.ru/bcode/467370

3. Корабельников, С. М. Преступления в сфере информационной безопасности: учебное пособие для вузов / С. М. Корабельников. – Москва: Издательство Юрайт, 2021. – 111 с. – (Высшее образование). – ISBN 978-5-534-12769-0. – URL: https://urait.ru/bcode/476798

4. Казарин, О. В. Надежность и безопасность программного обеспечения: учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. – Москва: Издательство Юрайт, 2021. – 342 с. – (Высшее образование). – ISBN 978-5-534-05142-1. – URL: https://urait.ru/bcode/473348

5. Гендина, Н. И. Информационная культура личности в 2 ч. Часть 1: учебное пособие для вузов / Н. И. Гендина, Е. В. Косолапова, Л. Н. Рябцева; под научной редакцией Н. И. Гендиной. – 2-е изд. – Москва: Издательство Юрайт, 2021; Кемерово: КемГИК. – 356 с. – (Высшее образование). – ISBN 978-5-534-14328-7 (Издательство Юрайт). – ISBN 978-5-8154-0518-9 (КемГИК). – URL: https://urait.ru/bcode/477568

6. Гендина, Н. И. Информационная культура личности в 2 ч. Часть 2: учебное пособие для вузов / Н. И. Гендина, Е. В. Косолапова, Л. Н. Рябцева; под научной редакцией Н. И. Гендиной. – 2-е изд. – Москва: Издательство Юрайт, 2021; Кемерово: КемГИК. – 308 с. – (Высшее образование). – ISBN 978-5-534-14419-2 (Издательство Юрайт). – ISBN 978-5-8154-0518-9 (КемГИК). – URL: https://urait.ru/bcode/477569

Интернет-источники

1. Сайт о программировании. [Электронный ресурс]. URL: https://metanit.com/web/php/3.4.php

2. Шестаков А.П. Учителям информатики и математики и их любознательным ученикам (дидактические материалы по информатике и математике). [Электронный ресурс]. URL: http://comp-science.narod.ru/

Отечественные периодические издания:

1 Журнал «Информационная безопасность» – URL: http://information-security.ru/articles2/allpubliks

2 Журнал «Защита информации. Инсайд» ***(****единственный в России периодический, научный, информационно-методический журнал в области защиты информации)* – URL: ***http://www.inside-zi.ru/***

Зарубежные периодические издания:

Открытые зарубежные периодические издания по информационной безопасности

Журнал https://www.infosecurity-magazine.com/

Журнал «(IN)SECURE Magazine» https://www.helpnetsecurity.com/insecuremag-archive/

Перечень профессиональных баз данных

1 Открытые профессиональные базы данных Федеральной службы техническому и экспортному контролю - «Банк данных угроз безопасности информации – URL: https://bdu.fstec.ru/threat/ ;
«Список уязвимостей» – URL: https://bdu.fstec.ru/vul

Перечень ресурсов информационно-телекоммуникационной сети Интернет, необходимых для освоения дисциплины
http://www.fsb.ru/ (сайт ФСБ России);
http://www.fstec.ru/ (сайт Федеральной службы по техническому и экспортному контролю (ФСТЭК России));
http://www.komitet2-16.km.duma.gov.ru/ (сайт комитета Государственной Думы по безопасности);
http://www.scrf.gov.ru/ (сайт Совета безопасности Российской Федерации);
http://www.mvd.ru/ (сайт Министерства внутренних дел (МВД России).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения обучающимися индивидуальных заданий, проектов, исследований.

Результаты обучения	**Коды формируемых профессиональных и общих компетенций**	**Формы и методы оценки**
Перечень умений, осваиваемых в рамках дисциплины: - использовать методы защиты программного обеспечения компьютерных систем; - анализировать риски и характеристики качества программного обеспечения; - выбирать и использовать методы и средства защиты компьютерных систем программными и аппаратными средствами; - применять стандартные методы для защиты объектов базы данных; - выполнять стандартные процедуры резервного копирования и мониторинга выполнения этой процедуры; - выполнять процедуру восстановления базы данных и вести мониторинг выполнения этой процедуры; - выполнять установку и настройку программного обеспечения для обеспечения работы пользователя с базой данных; - обеспечивать информационную безопасность на уровне базы данных. - основные понятия информационной безопасности; - источники возникновения информационных угроз; - модели и принципы защиты информации от несанкционированного доступа; - способы защиты информации в персональном компьютере; - методы криптографического преобразования информации; - методы антивирусной защиты информации; - состав и методы правовой защиты информации; - проблемы и направления развития системных программных средств.	ОК 01. ОК 02. ОК 04. ОК 05. ОК 09. ОК 10. ПК 1.4. ПК 4.5. ПК 4.6.	Опрос (устный/письменный) Тестирование. Оценка внеаудиторной самостоятельной работы. Подготовка и выступление с докладом/сообщением. Наблюдение за выполнением практического задания. (деятельностью студента) Оценка выполнения практического задания (работы). Решение ситуационной задачи.