приложение 2.8
к АОП по специальности
10.02.05 Обеспечение информационной
безопасности автоматизированных систем

АДАПТИРОВАННАЯ РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ ОПЦ.01 ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

для обучающихся с расстройством аутистического спектра

2024г.

Адаптированная рабочая программа учебной дисциплины разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупненной группы специальностей 10.00.00 Информационная безопасность для обучающихся с расстройством аутистического спектра.

.

Организация-разработчик: государственное бюджетное профессиональное образовательное учреждение Новосибирской области «Новосибирский профессионально-педагогический колледж»

Разработчик:
Волкова Н.И., преподаватель

Рассмотрена и принята на заседании кафедры информационных технологий и дизайна
Протокол № 1 от 29.08.2024г.

Руководитель кафедры _____ О.Ю.Ануфриева
(подпись)

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА АДАПТИРОВАННОЙ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ
«ОПЦ.01 Основы информационной безопасности»

1.1 Место дисциплины в структуре адаптированной образовательной программы

Учебная дисциплина «Основы информационной безопасности» является обязательной частью общепрофессионального цикла адаптированной образовательной программы в соответствии с ФГОС СПО по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, входящей в состав укрупненной группы специальностей 10.00.00 Информационная безопасность для обучающихся с расстройством аутистического спектра.

.

1.2 Цель и планируемые результаты освоения дисциплины

В рамках программы учебной дисциплины обучающимися осваиваются умения и знания

Код ПК, ОК	Умения	Знания
ОК 2 ОК 6 ОК 9 ПК 2.4	– классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации.	– сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины и виды учебной работы

Вид учебной работы	**Объем в часах**
Объем образовательной программы учебной дисциплины	60
в т.ч. в форме практической подготовки	18
в том числе:	
Лекции, уроки	34
практические занятия	18
Самостоятельная работа	4
Консультации	4
Промежуточная аттестация во 2 семестре в форме дифференцированного зачета	

2.2 Тематический план и содержание учебной дисциплины «Основы информационной безопасности»

Наименование разделов и тем	Содержание учебного материала и формы организации деятельности обучающихся	Объем в часах	Коды компетенций, формированию которых способствует элемент программы
1	2	3	4
Раздел 1. Теоретические основы информационной безопасности		**18**	
Тема 1.1 Основные понятия и задачи информационной безопасности	**Содержание учебного материала**	**6**	ОК 2, ОК 6, ОК 9 ПК 2.4
	Основные понятия информационной безопасности. История.	4	
	Основные виды и источники угроз информационной безопасности РФ.		
	Самостоятельная работа	**2**	
	Подготовка сообщения на тему: «Информационная война. Информационное оружие. Радиоэлектронная борьба»		
Тема 1.2 Основы защиты информации от угроз	**Содержание учебного материала**	**12**	ОК 2, ОК 6, ОК 9 ПК 2.4
	Целостность, доступность и конфиденциальность информации. Цели и задачи защиты.	8	
	Жизненные циклы конфиденциальной информации.		
	Классификация информации по видам тайны и степеням конфиденциальности (государственная тайна, конфиденциальная информация).		
	Интеграции информационной безопасности в деятельность организации.		
	В том числе практических занятий	**4**	
	ПР1 Подготовка доклада об охране различных видов тайн (государственной, коммерческой, банковской, профессиональной, служебной тайн, медицинской и персональных данных)	2	
Тема 1.3. Угрозы безопасности защищаемой информации	ПР2 Определение угроз объекта информатизации и их классификация	2	
Раздел 2. Методология защиты информации		**42**	
Тема 2.1. Методологические подходы к защите	**Содержание учебного материала**	**8**	ОК 2, ОК 6, **ОК 9** ПК 2.4
	В том числе практических занятий	**6**	
	ПР3 Работа в справочно-правовой системе с документами по информационной безопасности	2	

информации **Тема 2.2** Нормативно правовое регулирование защиты информации	ПР4 Авторское право и интеллектуальная собственность	2	
	ПР5 Система лицензирования и сертификации РФ в области защиты информации	2	
	Консультация	**2**	
Тема 2.3 Защита информации в автоматизированных (информационных) системах	**Содержание учебного материала**	**34**	ОК 2, ОК 6, ОК 9 ПК 2.4
	Элементы и объекты защиты. Методы, средства и механизмы защиты.	22	
	Технологии предотвращения угроз информационной безопасности.		
	Технологии парирования и нейтрализации угроз информационной безопасности.		
	Криптография. Классификация методов криптографического закрытия.		
	Шифрование различными методами. Кодирование.		
	Системы с открытыми ключами. Электронная цифровая подпись.		
	Классификация вирусов. Технологии борьбы.		
	Виды антивирусных программы. Плюсы и минусы.		
	Основные механизмы защиты ПК от несанкционированного доступа (физическая защита, аутентификация, разграничение доступа, криптографическое закрытие, регистрация обращений).		
	Инженерная защита и техническая охрана объектов информатизации.		
	Автоматизированные системы контроля доступа (АСКД) (использование пластиковых идентификационных карточек, смарт-карт, логотипов, эмбоссирования и биометрических систем идентификации).		
	В том числе практических занятий	**8**	
	ПР6 Выбор средств защиты информации, необходимых в колледже	2	
	ПР7 Расшифровка текста.	2	
	ПР8 Защита файлов и папок на персональном компьютере.	2	
	Дифференцированный зачет	2	
	Самостоятельная работа	**2**	
	Подготовка доклада на тему: «Современные системы контроля управления доступом».		
	Консультация	**2**	
Всего		**60**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1 Для реализации программы учебной дисциплины предусмотрены следующие специальные помещения:

Лаборатории информационных технологий, программирования и баз данных.

Оборудование лаборатории информационных технологий, программирования и баз данных:

- рабочие места на базе вычислительной техники по одному рабочему месту на
- обучающегося, подключенными к локальной вычислительной сети и сети «Интернет»;
- программное обеспечение сетевого оборудования;
- обучающее программное обеспечение.

.

3.1.1. Требования к материально-техническому обеспечению образовательной программы обучающихся с РАС

В учебных аудиториях (по возможности) стараться избегать использования ламп дневного света с дросселями, т.к. они мерцают и издают гул. Преимущественное использование светодиодов или ламп дневного света с качественным электронным балластом.

В аудиториях не должно быть гула или стробоскопического эффекта. Обеспечение хорошей акустики: не должно быть эха, посторонних шумов и т.п.

3.2 Информационное обеспечение реализации программы

Для реализации программы библиотечный фонд колледжа имеет печатные и/или электронные образовательные и информационные ресурсы, для использования в образовательном процессе. При формировании библиотечного фонда колледжем выбирается не менее одного издания из перечисленных ниже печатных изданий и (или) электронных изданий в качестве основного, при этом список, может быть дополнен новыми изданиями.

Обучающиеся инвалиды и лица с ограниченными возможностями здоровья обеспечены печатными и (или) электронными учебными изданиями, адаптированными при необходимости для обучения указанных обучающихся.

Обучающимся обеспечен доступ (удаленный доступ), в том числе в случае применения электронного обучения, дистанционных образовательных технологий, к современным профессиональным базам данных и информационным справочным системам, состав которых определяется настоящей адаптированной рабочей программой и подлежит обновлению (при необходимости).

3.2.2. Требования к учебно-методическому обеспечению образовательной программы для обучающихся с РАС

Предоставление презентаций, конспектов, видеозаписей занятий и т.п. Структурировано оформленные фонды оценочных средств. Дополнительные подробные инструкции и пояснения для выполнения задания.

3.2.1 Основные печатные издания

1. Бубнов, А. А. Основы информационной безопасности [Текст]: учебник/ А. А. Бубнов, В. Н. Пржегорлинский, О. А. Савинкин. - М.: Академия, 2020. - 256 с.: ил. - (Профессиональное образование).

2. Информационная безопасность: учебник / Мельников В.П., под ред., Куприянов А.И., Васильева Т.Ю. — Москва: КноРус, 2020. — 371 с. — (для бакалавров). — ISBN 978-5-406-07695-8. — URL: https://book.ru/book/932908 — Текст: электронный.

3.2.2 Дополнительные печатные источники

1. Волкова Н.И. Информационная безопасность: учебно-методическое пособие. - Новосибирск, 2019. – 56 с.

2. Мельников, В. П. Информационная безопасность [Текст]: учебное пособие/ В.П. Мельников, С.А. Клейманов, А.М. Петраков; под ред. С.А. Клейманов. - М.: Академия, 2021. - 333 с.: ил. - (Среднее профессиональное образование).

3. Партыка Т.Л., Попов И.И. Информационная безопасность [Текст]: учебное пособие для студентов учреждений среднего профессионального образования – 5-е изд., перераб. и доп. - М.: ФОРУМ: ИНФРА – М, 2020. – 432 с.: ил. – (Профессиональное образование).

4. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей [Текст]: учебное пособие - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2019. - 416 с. - (Профессиональное образование).

3.2.3 Периодические издания

1. Журналы Chip/Чип: Журнал о компьютерной технике для профессионалов и опытных пользователей;
2. Журналы Защита информации. Инсайд: Информационно-методический журнал
3. Информационная безопасность регионов: Научно-практический журнал
4. Вопросы кибербезопасности. Научный, периодический, информационно-методический журнал с базовой специализацией в области информационной безопасности.. URL: http://cyberrus.com/
5. Безопасность информационных технологий. Периодический рецензируемый научный журнал НИЯУ МИФИ. URL: http://bit.mephi.ru/

3.2.4 Дополнительные источники

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru
2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru
3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/
4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
5. Справочно-правовая система «Гарант» » www.garant.ru
6. Федеральный портал «Российское образование www.edu.ru
7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
8. Российский биометрический портал www.biometrics.ru
9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
10. Сайт Научной электронной библиотеки www.elibrary.ru

В условиях дистанционного обучения:

- инструктаж и выдача задания производится в форме телеконференции в Сферум;
- вся необходимая документация высылается по электронной почте;
- обратная связь и консультации осуществляются в приложении Вконтакте и по электронной почте;
- выполненные задания собираются в архив и отправляются на облако;
- экзамен осуществляется в форме телеконференции в Сферум.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Результаты обучения	Критерии оценки	Формы и методы оценки
Знания: – сущность и понятие информационной безопасности, характеристику ее составляющих; – место информационной безопасности в системе национальной безопасности страны; – виды, источники и носители защищаемой информации; – источники угроз безопасности информации и меры по их предотвращению; – факторы, воздействующие на информацию при ее обработке в автоматизированных (информационных) системах; – жизненные циклы информации ограниченного доступа в процессе ее создания, обработки, передачи; – современные средства и способы обеспечения информационной безопасности; – основные методики анализа угроз и рисков информационной безопасности.	Демонстрация знаний по курсу «Основы информационной безопасности» в повседневной и профессиональной деятельности.	Экспертная оценка результатов деятельности обучающегося при выполнении и защите результатов практических занятий. Тестирование Дифференцированный зачет
Умения: – классифицировать защищаемую информацию по видам тайны и степеням секретности; – классифицировать основные угрозы безопасности информации;	Умения проводить классификацию информации по видам тайны и степени секретности, основных угроз информации в профессиональной деятельности	Экспертное наблюдение в процессе практических занятий Дифференцированный зачет

Для осуществления процедур текущего контроля успеваемости, промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для обучающихся инвалидов и лиц с ограниченными возможностями здоровья, позволяющие оценить достижение ими результатов обучения и уровень сформированности всех компетенций, предусмотренных адаптированной образовательной программой.

Форма проведения текущей аттестации для обучающихся с ограниченными возможностями здоровья и инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа при прохождении аттестации.