АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ

СРЕДНЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

«ЦИФРОВОЙ КОЛЛЕДЖ «СИНЕРГИЯ»

РАБОЧАЯ ПРОГРАММА

учебной практики

УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами

для специальности *10.02.05 Обеспечение информационной безопасности автоматизированных систем*

(квалификация – техник по защите информации)

Якутск, 2023

СОГЛАСОВАНО
на заседании Педагогического совета
Протокол № 1 от «28» июня 2023 г.

УТВЕРЖДАЮ
Директор АНО СПО «Цифровой колледж «Синергия»
_____ С.Н.Семенов
«____» _____ 2023 г.

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 77940D002EB0E596473E4E262E45A5A4
Владелец: Семенов Семен Николаевич
Действителен: с 27.06.2023 до 27.06.2024

Рабочая программа учебной практики по УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами разработана на основе Федерального государственного образовательного стандарта среднего профессионального образования (далее – ФГОС СПО) *по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем,* утвержденного приказом Министерства образования и науки РФ от 9.12.2016 г. № 1553

Организация-разработчик: АНО СПО «Цифровой колледж «Синергия»

Составитель:

Сидорова А.Ю., зам.директора по УВР

СОДЕРЖАНИЕ

1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ПРАКТИКИ
УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами

1.1. Область применения рабочей программы

Рабочая программа учебной практики по УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами является частью основной профессиональной образовательной программы СПО – программы подготовки специалистов среднего звена по специальности *10.02.05 Обеспечение информационной безопасности автоматизированных систем (квалификация – техник по защите информации)***,** входящей в состав укрупненной группы специальностей *10.00.00 Информационная безопасность*.

1.2. Место учебной практики в структуре образовательной программы:

Учебная практика по УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами является частью профессионального модуля ПМ.02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами и проводится концентрировано.

1.3. Цели учебной практики – требования к результатам

Учебная практика направлена на формирование у обучающихся умений, приобретение практического опыта по ПМ.02. Защита информации в автоматизированных системах программными и программно-аппаратными средствами. Обучающийся должен

уметь:

$У_1$ - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;

$У_2$ - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации;

$У_3$ - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации;

$У_4$ - использовать типовые программные криптографические средства, в том числе электронную подпись;

$У_5$ - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями;

$У_6$ - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

иметь практический опыт в:

$ПО_1$ - установке и настройке программных средств защиты информации;

$ПО_2$ - тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;

$ПО_3$ - учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.

Результатом освоения учебной практики является овладение обучающимися основным видом деятельности – **ОВД.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами**, в том числе **профессиональными компетенциями (ПК):**

ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.

ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.

ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации.

ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.

ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

и **общими компетенциями (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 03. Планировать и реализовывать собственное профессиональное и личностное развитие.

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 06. *Проявлять гражданско-патриотическую позицию*[1], демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.

ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях.

ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.

ОК 09. Использовать информационные технологии в профессиональной деятельности.

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

ОК 11. *Использовать знания по финансовой грамотности*, планировать предпринимательскую деятельность в профессиональной сфере.

1.4. Количество часов на освоение учебной практик

Общее количество часов – 108 часов (3 недель),
в том числе в форме практической подготовки – 108 часов

1.5. Формы промежуточной аттестации

4 семестр – дифференцированный зачет (УП.02)

[1] Выделенное курсивом не формируется в рамках данной практики

2. ТЕМАТИЧЕСКИЙ ПЛАН И СОДЕРЖАНИЕ УЧЕБНОЙ ПРАКТИКИ

УП.02. Учебная практика по функционированию компьютерных сетей

Умения и практический опыт	Содержание учебной практики, виды работ, обеспечивающие формирование умений и приобретение практического опыта		Объем часов	В т.ч. практическая подготовка
уметь: $У_1$ - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; $У_2$ - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; $У_3$ - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; $У_4$ - использовать типовые программные криптографические средства, в том числе электронную подпись; $У_5$ - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; $У_6$ - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.	*Виды работ*			
	1	Знакомство с программой учебной практики, сроками и условиями выполнения работ. Требования охраны труда Ознакомление с планом проведения учебной практики.	2	2
	2	Установка операционной системы Windows XP на виртуальной машине Использование редактора реестра. Управление дисками из командной строки Обеспечение безопасности папок и документов Реализация подсистем аутентификации в распространенных операционных системах. Аудит в Windows. Просмотр и работа с журналом аудита «Противодействие взлому» «Работа со зловредными программами»	34	34
	3	Диагностика, устранение отказов и обеспечение работоспособности программно-аппаратных средств обеспечения информационной безопасности	12	12
	4	Оценка эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности	6	6
	5	Составление документации по учету, обработке, хранению и передаче конфиденциальной информации	6	6
	6	Анализ программного обеспечения для обработки, хранения и передачи конфиденциальной информации	6	6
	7	Составление маршрута и состава проведения различных видов контрольных проверок при аттестации объектов, помещений, программ, алгоритмов.	6	6

иметь практический опыт в: $ПО_1$ - установке и настройке программных средств защиты информации; $ПО_2$ - тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; $ПО_3$ - учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.	8	Устранение замечаний по результатам проверки	6	6
	9	Анализ и составление нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами, с учетом нормативных правовых актов.	12	12
	10	Применение математических методов для оценки качества и выбора наилучшего программного средства	6	6
	11	Использование типовых криптографических средств и методов защиты информации, в том числе и электронной подписи	6	6
	12	**Дифференцированный зачет**	**6**	6
		ВСЕГО:	**108**	**108**

3. УСЛОВИЯ РЕАЛИЗАЦИИ РАБОЧЕЙ ПРОГРАММЫ

3.1. Материально-техническое обеспечение

Реализация рабочей программы учебной практики УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами проходит в лаборатории Программных и программно-аппаратных средств обеспечения информационной безопасности.

Оборудование лаборатории:

- посадочные места по количеству обучающихся;
- проектор, экран;
- рабочее место преподавателя – АРМ преподавателя;
- персональные компьютеры на каждого обучающегося;
- программное обеспечение;
- аппаратное обеспечение.

Перечень программного обеспечения:

1. MS Windows 7
2. MS Office 2007
3. MS Windows 2003/2008
4. Autodesk AutoCAD 2019 Edu (свободное);
5. visual c++ 2008 express edition (свободное),
6. oracle vm virtualbox (свободное),
7. cisco packet tracer (свободное),
8. mocrosoft SQL server 2008 (свободное),
9. k-lite codec pack (свободное),
10. visual studio 2008 (свободное),

3.2 Информационное обеспечение обучения

Учебная литература:

Литература:

1. Васильева, И. Н. Криптографические методы защиты информации : учебник и практикум для вузов / И. Н. Васильева. — Москва : Издательство Юрайт, 2023. — 349 с. — (Высшее образование). — ISBN 978-5-534-02883-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/511890 (дата обращения: 09.07.2023).

2. 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, 2023. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/518005 (дата обращения: 09.07.2023).

3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для среднего профессионального образования / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2023. — 312 с. — (Профессиональное образование). — ISBN 978-5-534-13221-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/519364 (дата обращения: 09.07.2023).

Интернет - ресурсы

http://www.thg.ru/ - сеть изданий о современной электронике в мире;

http://www.linux.org.ru — сайт о разработках ОС Linux;

http://www.altlinux.ru - сайт компании ALT Linux - Российского лидера в разработке свободного ПО и дистрибутивов на базе Linux

Руководство по разработке структуры и проектированию баз данных – URL: https://www.internet-technologies.ru/articles/rukovodstvo-po-razrabotke-struktury-i-proektirovaniyu-bazy-dannyh.html

Дополнительная литература:

1. Погорелов Б.А., Сачков В.Н. (ред.). Словарь криптографических терминов. - М.: МЦНМО, 2006 Словарь криптографических терминов. Под ред. Б.А. Погорелова и В.Н. Сачкова. – М.: МЦНМО, 2006 г

2. Федеральный закон от 27 июля2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

4. Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

5. Федеральный закон от 4 мая 2011 г. № 99-ФЗ «О лицензировании отдельных видов деятельности».

6. Федеральный закон от 30 декабря 2001 г. № 195-ФЗ «Кодекс Российской Федерации об административных правонарушениях».

7. Указ Президента Российской Федерации от 16 августа 2004 г. № 1085 «Вопросы Федеральной службы по техническому и экспортному контролю».

8. Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера».

9. Указ Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена».

10. Положение о сертификации средств защиты информации. Утверждено постановлением Правительства Российской Федерации от 26 июня 1995 г. № 608.

11. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждены приказом ФСТЭК России от 18 февраля 2013 г. № 21.

12. Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

13. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по технической защите конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г.

14. Административный регламент ФСТЭК России по предоставлению государственной услуги по лицензированию деятельности по разработке и производству средств защиты конфиденциальной информации. Утвержден приказом ФСТЭК России от 12 июля 2012 г. № 84.

15. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). Утверждены приказом Гостехкомиссии России от 30 августа 2002 г. № 282.

16. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

17. Требования о защите информации, содержащейся в информационных системах общего пользования. Утверждены приказами ФСБ России и ФСТЭК России от 31 августа 2010 г. № 416/489.

18. Требования к системам обнаружения вторжений. Утверждены приказом ФСТЭК России от 6 декабря 2011 г. № 638

19. Руководящий документ. Геоинформационные системы. Защита информации от несанкционированного доступа. Требования по защите информации. Утвержден ФСТЭК России, 2008.

20. Руководящий документ. Защита от несанкционированного доступа к информации. Часть 2. Программное обеспечение базовых систем ввода-

вывода персональных электронно-вычислительных машин. Классификация по уровню контроля отсутствия недекларированных возможностей. Утвержден ФСТЭК России 10 октября 2007 г.

21. Приказ ФАПСИ при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

22. Приказ ФСБ России от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации».

23 ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий.

24 ГОСТ Р ИСО/МЭК ТО 13335-3-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 3. Методы менеджмента безопасности информационных технологий

25 ГОСТ Р ИСО/МЭК ТО 13335-4-2007 Информационная технология. Методы и средства обеспечения безопасности. Часть 4. Выбор защитных мер.

26 ГОСТ Р ИСО/МЭК ТО 13335-5-2006 Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.

27 ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.

28 ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.

29 ГОСТ Р ИСО/МЭК 15408-2-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.

30 ГОСТ Р ИСО/МЭК 15408-3-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.

31 ГОСТ Р 34.10-2001. "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи"

32 ГОСТ Р 34-11-94. "Информационная технология. Криптографическая защита информации. Функция хэширования"

33 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Ростехрегулирование, 2006

34 ГОСТ Р 52069.0-2013. Защита информации. Система стандартов. Основные положения. Росстандарт, 2013

35 ГОСТ Р 51583-2014. Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Росстандарт, 2014.

36 ГОСТ Р 51624-2000. Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования. Госстандарт России, 2000.

37 ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

38 ГОСТ Р 52447-2005. Защита информации. Техника защиты информации. Номенклатура показателей качества. Ростехрегулирование, 2005.

39 ГОСТ Р 50543-93. Конструкции базовые несущие. Средства вычислительной техники. Требования по обеспечению защиты информации и электромагнитной совместимости методом экранирования. Госстандарт России, 1993.

40 ГОСТ Р 56103-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Организация и содержание работ по защите от преднамеренных силовых электромагнитных воздействий. Общие положения. Росстандарт, 2014.

41 ГОСТ Р 56115-2014. Защита информации. Автоматизированные системы в защищенном исполнении. Средства защиты от преднамеренных силовых электромагнитных воздействий. Общие требования. Росстандарт, 2014.

42 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. Росстандарт, 2012.

43 ГОСТ Р ИСО/МЭК 15408-2-2013 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки

безопасности информационных технологий. Часть 2. Функциональные требования безопасности (прямое применение ISO/IEC 15408-2:2008). Росстандарт, 2013.

44 Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена ФСТЭК России 14 февраля 2008 г.

45 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

46 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Ростехрегулирование, 2006.

47 ГОСТ Р 51275-2006. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. Ростехрегулирование, 2006.

48 Сборник временных методик оценки защищенности конфиденциальной информации от утечки по техническим каналам. Утвержден Гостехкомиссией России, 2002.

49 Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах. Утверждены приказом ФСТЭК России от 11 февраля 2013 г. № 17.

50 Меры защиты информации в государственных информационных системах. Утверждены ФСТЭК России 11 февраля 2014 г.

51 Методические рекомендации по технической защите информации, составляющей коммерческую тайну. Утверждены ФСТЭК России 25 декабря 2006 г.

в) программное обеспечение: специализированное программное обеспечение для проверки защищенности помещений от утечки информации по акустическому и виброакустическому каналам, специальных исследований средств вычислительной техники;

г) базы данных, информационно-справочные и поисковые системы: www.fstec.ru ; www.gost.ru/wps/portal/tk362 .

3.3 Учебно-методическое обеспечение обучения

По учебной практике УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами создана учебно-методическая документация:

– Рабочая программа;

– Оценочные материалы;

– Методические указания по выполнению видов работ;
– Дидактический материал.

3.4. Общие требования к организации учебной практики

По результатам прохождения учебной практики обучающиеся сдают выполненные задания по видам работ.

Форма промежуточной аттестации – ***дифференцированный зачет.***

3.5. Кадровое обеспечение

Требования к квалификации педагогических кадров, осуществляющих руководство учебной практикой:

- учебная практика УП.02 проводится преподавателем, имеющим высшее образование, соответствующее профилю преподаваемого профессионального модуля. Опыт деятельности в организациях соответствующей профессиональной сферы является обязательным. Преподаватели получают дополнительное профессиональное образование по программам повышения квалификации, в том числе в форме стажировки в профильных организациях не реже 1 раза в 3 года.

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ

Контроль и оценка результатов выполнения работ обучающимися осуществляется преподавателем на занятиях по учебной практике.

Оценка качества освоения рабочей программы учебной практики обучающимся включает текущий контроль успеваемости и промежуточную аттестацию.

Код и наименование формируемых компетенций	***Практический опыт, умения, знания***	***Формы контроля и оценки результатов освоения***	
		Текущий контроль	***Промежуточная аттестация***
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации	**уметь:** $У_1$ - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; $У_5$ - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; **иметь практический опыт в:** $ПО_1$ - установке и настройке программных средств защиты информации;	- *комплексный контроль в ходе выполнения видов работ*	- *дифференцированный зачет*
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами	**уметь:** $У_2$ - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; $У_3$ - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; **иметь практический опыт в:** $ПО_2$ - тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;	- *комплексный контроль в ходе выполнения видов работ*	- *дифференцированный зачет*
ПК 2.3. Осуществлять тестирование функций отдельных программных и программно-	**уметь:** $У_2$ - диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-	- *комплексный контроль в ходе выполнения видов*	- *дифференцированный зачет*

Код и наименование формируемых компетенций	*Практический опыт, умения, знания*	*Формы контроля и оценки результатов освоения*	
		Текущий контроль	*Промежуточная аттестация*
аппаратных средств защиты информации	аппаратных средств защиты информации; $У_3$ - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; $У_6$ - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак **иметь практический опыт в:** $ПО_2$ - тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации;	*работ*	
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа	**уметь:** $У_6$ - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак **иметь практический опыт в:** $ПО_3$ - учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.	- *комплексный контроль в ходе выполнения видов работ*	- *дифференцированный зачет*
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств	**уметь:** $У_4$ - использовать типовые программные криптографические средства, в том числе электронную подпись; $У_5$ - устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; $У_6$ - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных	- *комплексный контроль в ходе выполнения видов работ*	- *дифференцированный зачет*

Код и наименование формируемых компетенций	*Практический опыт, умения, знания*	*Формы контроля и оценки результатов освоения*	
		Текущий контроль	*Промежуточная аттестация*
	средств обнаружения, предупреждения и ликвидации последствий компьютерных атак **иметь практический опыт в:** $ПО_3$ - учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.		
ПК 2.6. Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак	**уметь:** $У_6$ - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак **иметь практический опыт в:** $ПО_2$ - тестировании функций, диагностике, устранении отказов и восстановлении работоспособности программных и программно-аппаратных средств защиты информации; $ПО_3$ - учете, обработке, хранении и передаче информации, для которой установлен режим конфиденциальности.	- *комплексный контроль в ходе выполнения видов работ*	- *дифференцированный зачет*

Формы и методы контроля и оценки результатов обучения должны позволять проверять у обучающихся, не только сформированность профессиональных компетенций (ПК), но и общих компетенций (ОК):

Результаты (сформированные общие компетенции)	**Основные показатели оценки результата**	***Формы контроля и оценки результатов освоения***	
		Текущий контроль	***Промежуточная аттестация***
ОК 01. Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам	- самостоятельно организует свою деятельность по выданным заданиям ет оценить свои возможности для выполнения поставленных целей, задач, заданий по дисциплине	*комплексный контроль в ходе выполнения*	- *дифференцированный зачет*

ОК 02. Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности	- осуществляет поиск информации в сети Интернет и различных электронных носителях - извлекает информацию с электронных носителей - использует средства ИТ для обработки и хранения информации - представляет информацию в различных формах с использованием разнообразного программного обеспечения дает презентации в различных формах	*видов работ*	
ОК 03. Планировать и реализовывать собственное профессиональное и личностное развитие.	- берет на себя ответственность за принятое решение/совершенный поступок - ответственно выполняет разовые/ постоянные поручения в группе - может спрогнозировать результат - умеет оценить свои действия, поступки и проанализировать их		
ОК 04. Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами	- устанавливает позитивный стиль общения - выбирает стиль общения в соответствии с ситуацией - признает чужое мнение - при необходимости отстаивает собственное мнение - принимает критику - ведет деловую беседу в соответствии с этическими нормами - соблюдает официальный стиль при оформлении документов - выполняет письменные и устные рекомендации преподавателя - способен к эмпатии - организует коллективное обсуждение рабочей ситуации		
ОК 05. Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста	- умеет передавать информацию другому человеку - способен правильно формулировать свои мысли в устной и письменной формах - способен оценить уровень своих знаний по дисциплине		

ОК 06. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей, применять стандарты антикоррупционного поведения.	- не участвует в запрещенных группировках; - не проводит антироссийскую пропаганду; - уважительно относится к сверстникам, окружающим, старшим и младшим; - не хамит, не грубит - применяет в своем поведении стандарты антикоррупционного поведения		
ОК 07. Содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях	- поддерживает чистоту в учебном кабинете и на своем рабочем месте - адекватно реагирует на внезапное изменение ситуации (звонок, сирена, сигнал тревоги)		
ОК 08. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности.	- посещает учебные занятия, практику; - отсутствие пропусков по болезни - посещение спортивных секций в колледже и вне (по различным видам спорта)		
ОК 09. Использовать информационные технологии в профессиональной деятельности	- осуществляет поиск информации в сети Интернет и различных электронных носителях - извлекает информацию с электронных носителей - использует средства ИТ для обработки и хранения информации - представляет информацию в различных формах с использованием разнообразного программного обеспечения - создает презентации в различных формах		
ОК 10. Пользоваться профессиональной документацией на государственном и *иностранном* языках	- осуществлять эффективный поиск необходимой информации в российских и зарубежных источниках: нормативно-правовой документации, стандартов, научных публикации, технической документации; - уметь применять лексику и грамматику иностранного языка для перевода текста, содержание которого включает профессиональную лексику; - уметь анализировать, систематизировать и применять в		

	профессиональной деятельности информацию, содержащуюся в документации профессиональной области.		
ОК 11. Использовать знания по финансовой грамотности, планировать предпринимательскую деятельность в профессиональной сфере	- знает основную нормативную документацию по предпринимательской деятельности и может ее найти в поисковых системах; - определяет возможности/невозможности предпринимательства той или иной возникшей ситуации - - успешно учится, выполняет повседневные поручения/обязанности, связанные с финансами (оплата проезда, покупка продуктов, обеда) - владеет навыками обращения с банковскими картами		

Критерии и методы оценки сформированности умений и практического опыта отражены в Оценочных материалах учебной практики УП.02. Учебная практика по защите информации в автоматизированных системах программными и программно-аппаратными средствами.