Автономная некоммерческая организация высшего образования

«Российский новый университет»

Колледж

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ПРОИЗВОДСТВЕННОЙ (по профилю специальности) ПРАКТИКЕ

для специальности среднего профессионального образования

10.02.05 Обеспечение информационной безопасности автоматизированных систем

(базовая подготовка)

на базе среднего общего образования

Москва 2021

Одобрена
предметной (цикловой)
комиссией по специальности
09.02.05 Прикладная
информатика (по отраслям)

Разработана на основе Федерального государственного образовательного стандарта для специальности среднего профессионального образования 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденного приказом Министерства образования и науки Российской Федерации от 09.12.2016 № 1553, и учебного плана образовательной программы специалистов среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем.

Протокол № 08
от «26» мая 2021 г.

Председатель предметной
(цикловой) комиссии

_____/В.И. Аскерова

Заместитель директора колледжа по учебно-производственной работе

_____/Мальчевская И.Ю./

Составитель (автор): Аскерова В.И., преподаватель первой квалификационной категории колледжа АНО ВО «РосНОУ»

Рецензенты: Киркорова Н.И., генеральный директор ООО «Кибит», кандидат экономических наук, доцент

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по производственной (по профилю специальности) практике
10.02.05 Обеспечение информационной безопасности автоматизированных систем

Результаты обучения (освоенные умения, усвоенные знания)	ПК,ОК	Вид профессиональной деятельности	Уровень освоения	Формы и методы контроля
1	2	3	4	5
уметь: – обеспечивать работоспособность, обнаруживать и устранять неисправности, осуществлять комплектование, конфигурирование, настройку автоматизированных систем в защищенном исполнении и компонент систем защиты информации автоматизированных систем; – производить установку, адаптацию и сопровождение типового программного обеспечения, входящего в состав систем защиты информации автоматизированной системы; – организовывать, конфигурировать, производить монтаж, осуществлять диагностику и устранять неисправности компьютерных сетей, работать с сетевыми протоколами разных уровней; – настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам **знать:** – состав и принципы работы автоматизированных систем, операционных систем и сред; – принципы разработки алгоритмов программ, основных приемов программирования; – модели баз данных; – принципы построения, физические основы работы периферийных устройств; – теоретические основы компьютерных сетей и их аппаратных компонент, сетевых моделей, протоколов и принципов адресации; – порядок установки и ввода в эксплуатацию средств защиты информации в компьютерных сетях; – принципы основных методов организации и проведения технического обслуживания вычислительной техники и других технических средств информатизации.	ПК 1.1 – ПК 1.4 ОК 01 – ОК 10.	ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении	**3**	Зачет Характеристика о работе обучающегося по месту прохождения практики. Индивидуальное задание Дневник практики
уметь: - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации;	ПК 2.1 – ПК 2.6 ОК 01 – ОК 10	ПМ.02 Защита информации в автоматизированн	**3**	Зачет Характеристика о работе

- диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации; - проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; - применять математический аппарат для выполнения криптографических преобразований; - использовать типовые программные криптографические средства, в том числе электронную подпись; - применять средства гарантированного уничтожения информации; - устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; - осуществлять мониторинг и регистрацию сведений, необходимых для защиты объектов информатизации, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения. **знать:** - особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; - типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; - основные понятия криптографии и типовых криптографических методов и средств защиты информации; - особенности и способы применения программных и программно-аппаратных средств гарантированного уничтожения информации; - типовые средства и методы ведения аудита, средств и способов защиты информации в локальных вычислительных сетях, средств защиты от несанкционированного доступа.		ых системах программными и программно-аппаратными средствами		обучающегося по месту прохождения практики. Индивидуальное задание Дневник практики
уметь: – применять технические средства для криптографической защиты информации конфиденциального характера; – применять технические средства для уничтожения информации и носителей информации; – применять нормативные правовые акты, нормативные методические документы по обеспечению защиты информации техническими средствами; – применять технические средства для защиты информации в условиях применения мобильных устройств обработки и передачи данных;	ПК 3.1 – ПК 3.5 ОК 01 – ОК 10	ПМ.03 Защита информации техническими средствами	**3**	Зачет Характеристика о работе обучающегося по месту прохождения практики. Индивидуальное задание Дневник практики

– применять средства охранной сигнализации, охранного телевидения и систем контроля и управления доступом; – применять инженерно-технические средства физической защиты объектов информатизации **знать:** – порядок технического обслуживания технических средств защиты информации; – номенклатуру применяемых средств защиты информации от несанкционированной утечки по техническим каналам; – физические основы, структуру и условия формирования технических каналов утечки информации, способы их выявления и методы оценки опасности, классификацию существующих физических полей и технических каналов утечки информации; – порядок устранения неисправностей технических средств защиты информации и организации ремонта технических средств защиты информации; – методики инструментального контроля эффективности защиты информации, обрабатываемой средствами вычислительной техники на объектах информатизации; – номенклатуру и характеристики аппаратуры, используемой для измерения параметров ПЭМИН, а также параметров фоновых шумов и физических полей, создаваемых техническими средствами защиты информации; – основные принципы действия и характеристики технических средств физической защиты; – основные способы физической защиты объектов информатизации; – номенклатуру применяемых средств физической защиты объектов информатизации.				

Основные темы, закрепляемые в ходе прохождения производственной (по профилю специальности) практики

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении

МДК.01.01 Операционные системы

Тема 2.1. Принципы построения защиты информации в операционных системах

Понятие безопасности ОС. Классификация угроз ОС. Источники угроз информационной безопасности и объекты воздействия. Аутентификация, авторизация, аудит. Управление учетными записями пользователей и доступом к ресурсам. Аудит событий системы

Изучение штатных средств защиты информации в операционных системах

МДК.01.02 Базы данных

Тема 9.1. Обеспечение целостности, достоверности и непротиворечивости данных.

Угрозы целостности СУБД. Понятие хранимой процедуры. Достоинства и недостатки использования хранимых процедур. Понятие триггера.

Тема 9.2. Перехват исключительных ситуаций и обработка ошибок

Понятие исключительной ситуации. Мягкий и жесткий выход из исключительной ситуации. Место возникновения исключительной ситуации. Определение характера ошибки, вызвавшей исключительную ситуацию.

Тема 9.3. Механизмы защиты информации в системах управления базами данных

Средства идентификации и аутентификации. Общие сведения. Средства защиты информации в базах данных. Управление правами доступа к базам данных

Тема 9.4. Копирование и перенос данных. Восстановление данных

Создание резервных копий всей базы данных, журнала транзакций, а также одного или нескольких файлов или файловых групп. Аудит данных с помощью средств СУБД и триггеров. Резервное копирование и восстановление баз данных.

МДК.01.03 Сети и системы передачи информации

Тема 2.1. Архитектура и принципы работы современных сетей передачи данных

Структура и характеристики сетей. Способы коммутации и передачи данных. Распределение функций по системам сети и адресация пакетов. Маршрутизация и управление потоками в сетях связи. Протоколы и интерфейсы управления каналами и сетью передачи данных.

МДК.01.04 Эксплуатация автоматизированных (информационных) систем в защищенном исполнении

Тема 3.1. Основы информационных систем как объекта защиты

Понятие автоматизированной (информационной) системы. Отличительные черты АИС наиболее часто используемых классификаций: по масштабу, в зависимости от характера информационных ресурсов, по технологии обработки данных, по способу доступа, в зависимости от организации системы, по характеру использования информации, по сфере применения. Примеры областей применения АИС. Процессы в АИС: ввод, обработка, вывод, обратная связь. Требования к АИС: гибкость, надежность, эффективность, безопасность. Основные особенности современных проектов АИС. Электронный документооборот.

Тема 3.2. Жизненный цикл автоматизированных систем

Понятие жизненного цикла АИС. Процессы жизненного цикла АИС: основные, вспомогательные, организационные. Стадии жизненного цикла АИС: моделирование, управление требованиями, анализ и проектирование, установка и сопровождение. Модели жизненного цикла АИС. Задачи и этапы проектирования автоматизированных систем в защищенном исполнении. Методологии проектирования. Организация работ, функции заказчиков и разработчиков. Требования к автоматизированной системе в защищенном исполнении. Работы на стадиях и этапах создания автоматизированных систем в защищенном исполнении. Требования по защите сведений о создаваемой автоматизированной системе.

МДК.01.05. Эксплуатация компьютерных сетей

Тема 6.5. Адресация сетевого уровня и маршрутизация

Обзор адресации сетевого уровня. Формирование подсетей. Бесклассовая адресация IPv4. Способы конфигурации IPv4-адреса. Протокол IPv6. Формирование идентификатора интерфейса. Способы конфигурации IPv6-адреса. Планирование подсетей IPv6. Протокол NDP. Понятие маршрутизации. Дистанционно-векторные протоколы маршрутизации. Протокол RIP.

ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

МДК.02.01. **Программные и программно-аппаратные средства защиты информации**

Тема 1.3. Защищенная автоматизированная система

Автоматизация процесса обработки информации. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении. Методы создания безопасных систем. Методология проектирования гарантированно защищенных КС. Дискреционные модели. Мандатные модели. Тематика практических занятий и лабораторных работ. Учет, обработка, хранение и передача информации в АИС. Ограничение доступа на вход в систему. Идентификация и аутентификация пользователей. Разграничение доступа. Регистрация событий (аудит). Контроль целостности данных. Уничтожение остаточной информации. Управление политикой безопасности. Шаблоны безопасности. Криптографическая защита. Обзор программ шифрования данных.

Тема 2.1. Основы защиты автономных автоматизированных систем

Работа автономной АС в защищенном режиме. Алгоритм загрузки ОС. Штатные средства замыкания среды. Расширение BIOS как средство замыкания программной среды. Системы типа Электронный замок. ЭЗ с проверкой целостности программной среды. Понятие АМДЗ (доверенная загрузка). Применение закладок, направленных на снижение эффективности средств, замыкающих среду.

Тема 3.1. Основы построения защищенных сетей

Сети, работающие по технологии коммутации пакетов. Стек протоколов TCP/IP. Особенности маршрутизации. Штатные средства защиты информации стека протоколов TCP/IP. Средства идентификации и аутентификации на разных уровнях протокола TCP/IP, достоинства, недостатки, ограничения.

Тема 4.2. Защита информации в базах данных

Основные типы угроз. Модель нарушителя. Средства идентификации и аутентификации. Управление доступом. Средства контроля целостности информации в базах данных. Средства аудита и контроля безопасности. Критерии защищенности баз данных. Применение криптографических средств защиты информации в базах данных. Изучение механизмов защиты СУБД MS Access. Изучение штатных средств защиты СУБД MSSQL Server.

Тема 5.1. Мониторинг систем защиты

Понятие и обоснование необходимости использования мониторинга как необходимой компоненты системы защиты информации. Особенности фиксации событий, построенных на разных принципах: сети с коммутацией соединений, сеть с коммутацией пакетов, TCP/IP, X.25. Классификация отслеживаемых событий. Особенности построения систем мониторинга. Источники информации для мониторинга: сетевые мониторы, статистические характеристики трафика через МЭ, проверка ресурсов общего пользования. Классификация сетевых мониторов. Системы управления событиями информационной безопасности (SIEM). Обзор SIEM-систем на мировом и российском рынке.

МДК.02.02. Криптографические средства защиты информации

Тема 3.4. Аутентификация данных. Электронная подпись

Аутентификация данных. Общие понятия. ЭП. MAC. Однонаправленные хеш-функции. Алгоритмы цифровой подписи Применение различных функций хеширования, анализ особенностей хешей. Применение криптографических атак на хеш-функции. Изучение программно-аппаратных средств, реализующих основные функции ЭП.

Тема 3.6. Криптозащита информации в сетях передачи данных

Абонентское шифрование. Пакетное шифрование. Защита центра генерации ключей. Криптомаршрутизатор. Пакетный фильтр. Криптографическая защита беспроводных соединений в сетях стандарта 802.11 с использованием протоколов WPA, WEP.

ПМ.03 Защита информации техническими средствами

МДК.03.01 Техническая защита информации

Тема 2.2. Технические каналы утечки информации

Понятие и особенности утечки информации. Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика.

Тема 2.3. Методы и средства технической разведки

Классификация технических средств разведки. Методы и средства технической разведки. Средства несанкционированного доступа к информации. Средства и возможности оптической разведки. Средства дистанционного съема информации.

Тема 4.4. Системы защиты от утечки информации по электромагнитному каналу

Прослушивание информации от радиотелефонов. Прослушивание информации от работающей аппаратуры. Прослушивание информации от

радиозакладок. Приемники информации с радиозакладок. Прослушивание информации о пассивных закладках. Системы защиты от утечки по электромагнитному каналу. Номенклатура применяемых средств защиты информации от несанкционированной утечки по электромагнитному каналу. Определение каналов утечки ПЭМИН. Защита от утечки по цепям электропитания и заземления.

Тема 4.5. Системы защиты от утечки информации по телефонному каналу

Контактный и бесконтактный методы съема информации за счет непосредственного подключения к телефонной линии. Использование микрофона телефонного аппарата при положенной телефонной трубке. Утечка информации по сотовым цепям связи. Номенклатура применяемых средств защиты информации от несанкционированной утечки по телефонному каналу. Технические средства защиты информации в телефонных линиях.

Тема 5.1. Применение технических средств защиты информации

Технические средства для уничтожения информации и носителей информации, порядок применения. Порядок применения технических средств защиты информации в условиях применения мобильных устройств обработки и передачи данных. Проведение измерений параметров побочных электромагнитных излучений и наводок, создаваемых техническими средствами защиты информации, при проведении аттестации объектов. Применение технических средств защиты информации.

МДК.03.02 Инженерно-технические средства физической защиты объектов информатизации

Тема 2.1 Система обнаружения комплекса инженерно-технических средств физической защиты

Информационные основы построения системы охранной сигнализации. Назначение, классификация технических средств обнаружения. Построение систем обеспечения безопасности объекта. Периметровые средства обнаружения: назначение, устройство, принцип действия. Объектовые средства обнаружения: назначение, устройство, принцип действия. Монтаж датчиков пожарной и охранной сигнализации.

Тема 2.4. Система сбора, обработки, отображения и документирования информации

Классификация системы сбора и обработки информации. Схема функционирования системы сбора и обработки информации. Варианты структур построения системы сбора и обработки информации. Устройства

отображения и документирования информации. Рассмотрение принципов устройства, работы и применения системы сбора и обработки информации.

Тема 3.2. Эксплуатация инженерно-технических средств физической защиты

Этапы эксплуатации. Виды, содержание и порядок проведения технического обслуживания инженерно-технических средств физической защиты. Установка и настройка периметровых и объектовых технических средств обнаружения, периферийного оборудования системы телевизионного наблюдения. Диагностика, устранение отказов и восстановление работоспособности технических средств физической защиты. Организация ремонта технических средств физической защиты.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на производственную (по профилю специальности) практику

ПМ.01 Эксплуатация автоматизированных (информационных) систем в защищённом исполнении

При прохождении практики выполнить следующие задания:

- Заполнять ежедневно дневник о ходе прохождения учебной практики;
- Выполнить задание и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»).

1. Участие в установке и настройке компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации
2. Обслуживание средств защиты информации прикладного и системного программного обеспечения
3. Настройка программного обеспечения с соблюдением требований по защите информации
4. Настройка средств антивирусной защиты для корректной работы программного обеспечения по заданным шаблонам
5. Инструктаж пользователей о соблюдении требований по защите информации при работе с программным обеспечением
6. Настройка встроенных средств защиты информации программного обеспечения
7. Проверка функционирования встроенных средств защиты информации программного обеспечения
8. Своевременное обнаружение признаков наличия вредоносного программного обеспечения
9. Обслуживание средств защиты информации в компьютерных системах и сетях
10. Обслуживание систем защиты информации в автоматизированных системах
11. Участие в проведении регламентных работ по эксплуатации систем защиты информации автоматизированных систем
12. Проверка работоспособности системы защиты информации автоматизированной системы
13. Контроль соответствия конфигурации системы защиты информации автоматизированной системы ее эксплуатационной документации

14. Контроль стабильности характеристик системы защиты информации автоматизированной системы

15. Ведение технической документации, связанной с эксплуатацией систем защиты информации автоматизированных систем

16. Участие в работах по обеспечению защиты информации при выводе из эксплуатации автоматизированных систем

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на производственную (по профилю специальности) практику
ПМ.02 Защита информации в автоматизированных системах программными и программно-аппаратными средствами

При прохождении практики выполнить следующие задания:

- Заполнять ежедневно дневник в ходе прохождения учебной практики
- Выполнить задания и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»).

1. Анализ принципов построения систем информационной защиты производственных подразделений.
2. Техническая эксплуатация элементов программной и аппаратной защиты автоматизированной системы.
3. Участие в диагностировании, устранении отказов и обеспечении работоспособности программно-аппаратных средств обеспечения информационной безопасности;
4. Анализ эффективности применяемых программно-аппаратных средств обеспечения информационной безопасности в структурном подразделении
5. Участие в обеспечении учета, обработки, хранения и передачи конфиденциальной информации
6. Применение нормативных правовых актов, нормативных методических документов по обеспечению информационной безопасности программно-аппаратными средствами при выполнении задач практики.

ИНДИВИДУАЛЬНОЕ ЗАДАНИЕ
на производственную (по профилю специальности) практику
ПМ.03 Защита информации техническими средствами

При прохождении практики выполнить следующие задания:

- Заполнять ежедневно дневник в ходе прохождения учебной практики

- Выполнить задания и оформить результаты в печатном варианте с помощью MS Word (при необходимости можно использовать предоставления результатов работы «скриншоты»).

1. Участие в монтаже, обслуживании и эксплуатации технических средств защиты информации;
2. Участие в монтаже, обслуживании и эксплуатации средств охраны и безопасности, инженерной защиты и технической охраны объектов, систем видеонаблюдения;
3. Участие в монтаже, обслуживании и эксплуатации средств защиты информации от несанкционированного съёма и утечки по техническим каналам;
4. Применение нормативно правовых актов, нормативных методических документов по обеспечению защиты информации техническими средствами

Критерии оценок

В процессе прохождения производственной (по профилю специальности) практики контролируются и оцениваются уровень сформированности показателей профессиональной компетенции, а также полнота и качество представленных отчетных документов.

Промежуточная аттестация по дисциплине проходит в форме защиты отчета о прохождении практики (дифференцированного зачета).

Защита практики (дифференцированный зачет) проводится согласно расписанию зачетно-экзаменационной сессии.

К промежуточной аттестации не допускаются обучающиеся, не сдавшие отчет о прохождении практики.

При защите практики все обучающиеся размещаются в аудитории.

В ходе защиты преподаватель и присутствующие в аудитории обучающиеся могут задавать уточняющие и дополнительные вопросы.

Защита практики включает в себя:

1) доклад обучающегося о прохождении практики,
2) анализ выполнения индивидуальных заданий на практику и анализа и оценки действий обучающегося в ходе практики,
3) ответы обучающегося на вопросы руководителя практики от образовательной организации и других обучающихся.

В зависимости от результатов защиты руководителя практики от образовательной организации выставляет обучающемуся оценку в соответствии со следующими критериями:

Обучающийся, не выполнивший программу практики и получивший неудовлетворительную оценку при защите отчета, считается имеющим академическую задолженность.

В случае неполного выполнения обучающимся задания на

производственную (по профилю специальности) практику по уважительной причине приказом директора может быть дано разрешение на повторное её прохождение в свободное от образовательного процесса время.

После защиты отчетов по производственной практике руководитель обязан сдать отчеты на кафедру.

Оценка	Критерии оценки показателя компетенции
Зачтено-Отлично	- даны исчерпывающие и обоснованные ответы на все поставленные вопросы; - правильно выполнены все практические задания на практику; -представленный отчет соответствует установленным требованиям.
Зачтено-Хорошо	- даны полные, достаточно обоснованные ответы на поставленные вопросы, при ответах не всегда выделялось главное; - без ошибок выполнено более 75% практических заданий на практику; - представленный отчет соответствует установленным требованиям.
Зачтено-Удовлетворительно	- даны в основном правильные ответы на все поставленные вопросы, но без должной глубины и обоснования; - без ошибок выполнены не менее половины практических заданий на практику; - представленный отчет соответствует установленным требованиям.
Не зачтено-Неудовлетворительно	- не выполнены требования, предъявляемые к показателям компетенции, оцениваемым удовлетворительно, либо отсутствует отчет о прохождении практики, выполненный в соответствии с установленными требованиями.

Обучающийся, не выполнивший программу практики и получивший неудовлетворительную оценку при защите отчета, считается имеющим академическую задолженность.

В случае неполного выполнения обучающимся задания по производственной практике по уважительной причине приказом директора может быть дано разрешение на повторное её прохождение в свободное от образовательного процесса время.

После защиты отчетов по производственной (по профилю специальности) практике руководитель обязан сдать отчеты на кафедру.