МИНИСТЕРСТВО ОБРАЗОВАНИЯ БЕЛГОРОДСКОЙ ОБЛАСТИ
ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ОГАПОУ «АЛЕКСЕЕВСКИЙ КОЛЛЕДЖ»

Подписано цифровой подписью: Афанасьева Ольга Валерьевна
DN: cn=Афанасьева Ольга Валерьевна, o=ОГАПОУ "Алексеевский колледж", ou=Директор, email=afanasjeva_o@alcollege.ru, c=RU
Дата: 2024.01.23 00:52:58 +03'00'

УТВЕРЖДАЮ:
Директор ОГАПОУ
«Алексеевский колледж»

_____ / Афанасьева О.В.
Приказ № 662 от «05» июля 2023 года

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА

ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

«Основы информационной безопасности»

г. Алексеевка, 2023 г.

ОГЛАВЛЕНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

1.1. Цель реализации программы

Целью реализации программы повышения квалификации является обучение лиц, *обеспечению безопасности информации в компьютерных системах и сетях в условиях существования угроз их информационной безопасности*, в целях последовательного совершенствования профессиональных знаний, умений и навыков с учетом требований квалификационных характеристик, профстандарта *Специалист по безопасности компьютерных систем и сетей (рег.номер 842, утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14.09.2022 № 533н).*

Контроль и оценка результатов освоения курса осуществляется преподавателем в процессе проведения практических занятий, тестирования, а также выполнения слушателями курса индивидуальных заданий, исследований.

1.2. Планируемые результаты обучения

Формируемые компетенции:

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

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 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.

ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.

ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.

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.

Должен знать: основные принципы правового регулирования в области обработки и защиты информации, видов тайн, принципов обработки персональных данных, меры обеспечения безопасности персональных данных, последовательности действий по защите информации, подходов к моделированию нарушителей и угроз информационной безопасности, требования законодательства Российской Федерации о защите персональных данных; методы и средства защиты информации.

Должен уметь: настраивать и устранять неисправности программно-аппаратных средств защиты информации в компьютерных сетях по заданным правилам**,** обеспечивать работоспособность, обнаруживать и устранять неисправности

Должен овладеть навыками обеспечения защиты информации в автоматизированных системах отдельными программными, программно-аппаратными средствами; осуществлять обработку, хранение и передачу информации ограниченного доступа; уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.

1.3. Категория обучающихся

Дополнительная профессиональная программа повышения квалификации «Основы информационной безопасности» направлена на

формирование digital-competence, обеспечивающих осознанное применение цифровых технологий в обучении, в профессиональной деятельности и общественной жизни, владение методами защиты персональной информации и данных. Программа повышения квалификации ориентирована на широкий круг лиц, сталкивающихся с необходимостью повышения уровня личной информационной безопасности и уровня информационной безопасности небольшого предприятия или организации.

Направленность: отраслевая, под заказ работодателя, разработано для граждан предпенсионного возраста, разработано для учащихся общеобразовательных организаций, для получения первой профессии)

К освоению программы допускаются лица различного возраста, без предъявления требований к уровню образования.

Для освоения дополнительной профессиональной программы повышения квалификации «Основы информационной безопасности» необходимы начальные знания, умения и навыки в направлении информационных и коммуникационных технологий.

1.4. Нормативно-правовые основания разработки программы

Нормативно-правовую основу разработки программы составляют:

1) Федеральный закон Российской Федерации от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;

2) Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

3) Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»;

4) Перечень профессий рабочих, должностей служащих, по которым осуществляется профессиональное обучение, утвержденный приказом Министерства образования и науки РФ от 02.07.2013 № 513;

5) Приказ Министерства просвещения РФ от 26 августа 2020 г. № 438 «Об утверждении Порядка организации и осуществления

образовательной деятельности по основным программам профессионального обучения»;

6) Профессиональный стандарт *«Специалист по безопасности компьютерных систем и сетей»,* утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 14 сентября 2022г. №533Н;

7) Федерального государственного образовательного стандарта среднего профессионального образования по специальности 10.02.05 Обеспечение информационной безопасности автоматизированных систем, утвержденный приказом Министерства образования и науки Российской Федерации от 9 декабря 2016 года № 1553 (зарегистрирован Министерством юстиции Российской Федерации 26 декабря 2016 года, регистрационный № 44938).

1.5. Трудоемкость обучения

Срок обучения -72 часа.

1.6. Форма обучения

Форма обучения очно-заочная, с применением электронного обучения и дистанционных образовательных технологий. Программа может быть реализована дистанционно (электронный учебный курс), с использованием ЭО и ДОТ.

1.7. Итоговая аттестация

В Программе активно используются лабораторные работы, что позволяет слушателям не только в теории освоить материал Программы, но и на практике сразу отработать приобретенные навыки и закрепить полученные знания.

Оценка качества освоения программы производится с использованием контрольно-измерительных материалов, представленных в электронном

учебном курсе. Для отработки практических навыков в курс включены лабораторные работы. Для оценивания результатов освоения курса используются тестовые задания.

По результатам освоения программы дополнительного профессионального обучения выдается удостоверение о повышении квалификации установленного образца.

2. СОДЕРЖАНИЕ ПРОГРАММЫ

2.1. Учебный план

№ п/п	Наименование модуля (дисциплины)	Общая трудоемкость, (час.)	Всего аудиторных занятий, (час.)		Учебная практика, (час.)	Самостоятельная работа, (час.)	Дистанционное обучение, (час.)	Форма контроля
			Теоретические	Практические				
	Модуль № 1 «Правовые и организационные основы обеспечения информационной безопасности в Российской Федерации»							
1.1	Правовые основы обеспечения информационной безопасности	4	2	2		2		
1.2	Защита персональных данных	4	2	2				
1.3	Организационные основы обеспечения информационной безопасности	4	2	2				
	Промежуточная аттестация (ПА) по модулю 1							**зачет**
	Итого по модулю 1:	**12**						
	Модуль № 2 «Архитектура компьютера»							
2.1	Введение в архитектуру компьютера	2	1	1				
	Промежуточная аттестация (ПА) по модулю 2							**зачет**
	Итого по модулю 2:	**2**						
	Модуль № 3 «Технические каналы утечки информации»							
3.1	Понятие и особенности утечки информации	4	2	2				
	Промежуточная аттестация (ПА) по модулю 3							**зачет**
	Итого по модулю 3:	**4**						
	Модуль № 4 «Основы информационной безопасности в операционных системах»							
4.1	Введение в информационную безопасность операционных систем	2	2					
4.2	Информационная безопасность операционных систем	14		14				

	семейства Windows							
4.3	Информационная безопасность операционных систем семейства Linux	2	2					
	Промежуточная аттестация (ПА) по модулю 4							**зачет**
	Итого по модулю 4:	**18**						
Модуль № 5 «Основы информационной безопасности в локальных и глобальных компьютерных сетях»								
5.1	Применение локальных вычислительных сетей	4	2	2				
5.2	Применение глобальных вычислительных сетей	18		18				
5.3	Разработка мер и выбор средств обеспечения информационной безопасности локальной вычислительной сети	2		2				
	Промежуточная аттестация (ПА) по модулю 5							**зачет**
	Итого по модулю 5:	**24**						
Модуль № 6 «Основные компоненты комплекса инженерно-технических средств физической защиты»								
6.1	Система обнаружения комплекса инженерно-технических средств физической защиты	4	2	2				
	Промежуточная аттестация (ПА) по модулю 6							**зачет**
	Итого по модулю 6:	**4**						
Модуль № 7 «Криптографические методы защиты информации»								
7.1	Введение в криптографические методы защиты информации	4	2	2				
	Промежуточная аттестация (ПА) по модулю 7							**зачет**
	Итого по модулю 7:	**4**						
	Итоговая аттестация	**4**						**Квалификационный экзамен**
	Всего:	**72**						

2.2. Календарный учебный график[1]

Наименование разделов, дисциплин, модулей, практик	1 месяц				2 месяц				Всего часов обяз.уч.
	1 нед	2 нед	3 нед	4 нед	1 нед	2 нед	3 нед	4 нед	
Модуль № 1 «Правовые и организационные основы обеспечения информационной безопасности в Российской Федерации»	9	3							12
Модуль № 2 «Архитектура компьютера»		2							2
Модуль № 3 «Технические каналы утечки информации»		4							4
Модуль № 4 «Основы информационной безопасности в операционных системах»			9	9					18
Модуль № 5 «Основы информационной безопасности в локальных и глобальных компьютерных сетях»					9	9	6		24
Модуль № 6 «Основные компоненты комплекса инженерно-технических средств физической защиты»							3	1	4
Модуль № 7 «Криптографические методы защиты информации»								4	4
Квалификационный экзамен								**4**	**4**
всего часов									**72**

[1] Даты обучения будут определены в расписании занятий при наборе группы на обучение

2.3. Рабочие программы модулей (дисциплин)

Наименование модулей (дисциплин)	**Содержание обучения (по темам в дидактических единицах), наименование и тематика лабораторных работ, учебной практики, используемых образовательных технологий и рекомендуемой литературы лабораторных работ, практических занятий (семинаров), самостоятельной работы, используемых образовательных технологий и рекомендуемой литературы**
Модуль № 1 «Правовые и организационные основы обеспечения информационной безопасности в Российской Федерации»	
Тема 1.1. Правовые основы обеспечения информационной безопасности	Основные права граждан в сфере обработки и защиты информации. Основные принципы правового регулирования в области обработки и защиты информации. Информация. Основные свойства безопасности информации: конфиденциальность, целостность, доступность. Виды информации по порядку доступа и распространения. Ограничение доступа к информации. Виды тайн. Обладатель информации. Информационные технологии. Информационные системы. Оператор информационной системы. Защита информации. Объекты защиты. Виды ответственности в сфере обработки и защиты информации.
Практическая работа	*Уметь осуществлять поиск информации регламентирующей обеспечение информационной безопасности.*
Тема 1.2 Защита персональных данных	Персональные данные и принципы их обработки. Виды персональных данных: специальные, биометрические и общедоступные. Условия обработки персональных данных. Согласие на обработку персональных данных. Трансграничная передача персональных данных. Права субъектов персональных данных. Оператор персональных данных и его обязанности. Меры обеспечения безопасности персональных данных. Контроль и надзор за выполнением мер по обеспечению безопасности. Уполномоченный орган по защите прав субъектов персональных данных. Уничтожение информации и носителей информации с использованием программных и программно-аппаратных средств.
Практическая работа	*Уметь осуществлять поиск информации регламентирующей обеспечение информационной безопасности, ограничение доступа к информации.*
Тема 1.3 Организационные основы обеспечения информационной безопасности	Какие вопросы ставит информационная безопасность? Последовательность действий по защите информации. Выявление и анализ информационных активов. Формирование требований по защите информации. Подходы к моделированию нарушителей и угроз информационной безопасности. Выбор средств и методов защиты информации. Внедрение системы защиты информации. Эксплуатация системы защиты информации.
Практическая работа	*Уметь реализовать последовательность действий, направленную на защиту информации,*

	осуществлять выбор средств и методов по защите информации.
Модуль № 2 «Архитектура компьютера»	
Тема 2.1. Введение в архитектуру компьютера	Процессоры. Основная (кэш и оперативная) память. Вспомогательная память. Устройства ввода-вывода (шины, мониторы, клавиатуры и мыши, веб-камеры, принтеры). Персональные компьютеры и мобильные устройства
Практическая работа	*Уметь определить составляющие компьютера, осуществлять оптимизацию аппаратных и программных средств для автоматизации рабочего места пользователя.*
Модуль № 3 «Технические каналы утечки информации»	
Тема 3.1 Понятие и особенности утечки информации	Структура канала утечки информации. Классификация существующих физических полей и технических каналов утечки информации. Характеристика каналов утечки информации. Классификация демаскирующих признаков. Основные виды угроз информации. Организация обработки, хранения и передачи информации ограниченного доступа.
Практическая работа	*Уметь определить каналы утечки информации, виды угроз.*
Модуль № 4 «Основы информационной безопасности в операционных системах»	
Тема 4.1. Введение в информационную безопасность операционных систем	Общий способ хранения и обработки информации в компьютере. Понятия операционной и файловой систем. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Дискреционное управление доступом, мандатное управление доступом. Идентификация, аутентификация и авторизация. Аутентификация на основе паролей, на основе внешних носителей ключа, биометрическая аутентификация. Организация регистрации основных событий в автоматизированных системах.
Практическая работа	*Уметь организовать безопасный доступ для обработки и хранения информации на рабочем месте.*
Тема 4.2 Информационная безопасность операционных систем семейства Windows	Управление доступом в операционных системах семейства Windows. Идентификация, аутентификация и авторизация в операционных системах семейства Windows. Реализация аудита в операционных системах семейства Windows. Восстановление данных.
Практическая работа	*Уметь организовать безопасный доступ для обработки и хранения информации на рабочем месте, осуществлять проверку безопасных условий для работы в операционной системе и восстанавливать данные.*
Тема 4.3 Информационная безопасность операционных систем семейства Linux	Управление доступом в операционных системах семейства Linux. Идентификация, аутентификация и авторизация в операционных системах семейства Linux. Реализация аудита в операционных системах семейства Linux.
Практическая работа	*Уметь организовать безопасный доступ для обработки и хранения информации на рабочем месте.*

Модуль № 5 «Основы информационной безопасности в локальных и глобальных компьютерных сетях»	
Тема 5.1 Применение локальных вычислительных сетей	Локальные вычислительные сети. Основные функции локальных-вычислительных сетей. Анализ возможных атак.
Практическая работа	*Уметь организовать безопасный доступ для обработки и хранения информации на рабочем месте при работе в локальной сети.*
Тема 5.2 Применение глобальных вычислительных сетей	Глобальные вычислительные сети. Основные функции глобальных компьютерных сетей. Анализ возможных атак.
Практическая работа	*Уметь организовать безопасный доступ для обработки и хранения информации на рабочем месте при работе в глобальной вычислительной сети.*
Тема 5.3 Разработка мер и выбор средств обеспечения информационной безопасности локальной вычислительной сети	Признаки присутствия вредоносного программного обеспечения. Методы обнаружения. Организационные меры защиты. Составления плана защиты кабинета.
Практическая работа	*Уметь обнаружить и составить план обеспечения защиты автоматизированного рабочего места.*
Модуль №6 «Основные компоненты комплекса инженерно-технических средств физической защиты»	
Тема 6.1 Система обнаружения комплекса инженерно-технических средств физической защиты	Система контроля и управления доступом. Система телевизионного наблюдения. Система сбора, обработки, отображения и документирования информации. Система воздействия.
Практическая работа	*Уметь определить возможности повышения эффективности световых устройств.*
Модуль № 7 «Криптографические методы защиты информации»	
Тема 7.1. Введение в криптографические методы защиты информации	Исторический очерк развития криптографии. Симметричная и асимметричная криптография. Вычислительно сложные задачи математики. Криптосистема RSA. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Схемы цифровой подписи.
Практическая работа	*Уметь определить случаи для применения криптографических методов защиты информации.*
Используемые образовательные технологии	*Кейс-технологии – технология, которая основана на комплектовании учебно-методических материалов и предоставлении их слушателям для самостоятельного изучения и решения.* *Объяснительно-иллюстративные технологии – технологии, при которых объяснение учебного материала сопровождается различными наглядными средствами, сочетая с интерактивными средствами в виде презентаций, флеш-анимации, учебных фильмов, иструкционно-технологических карт и т.д.* *Проблемное обучение - создание в учебной деятельности проблемных ситуаций и*

	организация активной самостоятельной деятельности учащихся по их разрешению, в результате чего происходит творческое овладение знаниями, умениями, навыками, развиваются мыслительные способности.
Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы	Белов Е. Б. Основы информационной безопасности. Учебное пособие для вузов / Е. Б. Белов, В. П. Лось, Р. В. Мещеряков, А. А. Шелупанов. — М.: Горячая линия – Телеком, 2006. — 544 с. Таненбаум Э. Архитектура компьютера. 6-е изд / Э. Таненбаум, Т. Остин. — СПб.: Питер, 2013. — 816 с. Таненбаум Э. Современные операционные системы / Э. Таненбаум, Х. Бос. — СПб.: Питер, 2018. — 1120 с. Проскурин В. Г. Защита в операционных системах. Учебное пособие / В. Г. Проскурин. — М.: Горячая линия – Телеком, 2014. — 192 с. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы. Учебник для вузов / В. Г. Олифер, Н. А. Олифер. — СПб.: Питер, 2020. — 1008 с. Олифер В. Г. Безопасность компьютерных сетей. Учебное пособие для вузов / В. Г. Олифер, Н. А. Олифер. — М.: Горячая линия – Телеком, 2017. — 644 с. Ященко В.В. Введение в криптографию / Под общ. ред. В.В. Ященко. — 4-е изд. доп. М.: МЦНМО, 2012. — 348. 8. Алферов А.П. Основы криптографии. Учебное пособие / А. П. Алферов, А. Ю. Зубов, А. С. Кузьмин, А. В. Черемушкин — М.: Гелиос АРВ, 2001. — 480 с Электронные источники: Бекетнова, Ю. М. Международные основы и стандарты информационной безопасности финансово-экономических систем : учебное пособие / Ю. М. Бекетнова, Г. О. Крылов, С. Л. Ларионова. — Москва : Прометей, 2018. — 174 с. — ISBN 978-5-907003-27-9. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/94454 (дата обращения: 30.09.2022). — Режим доступа: для авторизир. Пользователей Филиппов, Б. И. Информационная безопасность. Основы надежности средств связи : учебник / Б. И. Филиппов, О. Г. Шерстнева. — Саратов : Ай Пи Эр Медиа, 2019. — 227 с. — ISBN 978-5-4486-0485-0. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/80290 (дата обращения: 30.09.2022). — Режим доступа: для авторизир. Пользователей Масюк, М. А. Основные понятия и правовые основы защиты информации : учебное пособие / М. А. Масюк, А. А. Попов, Е. В. Касьянова. — Красноярск : Сибирский

	государственный университет науки и технологий имени академика М.Ф. Решетнева, 2020. — 82 с. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/116643 (дата обращения: 30.09.2022). — Режим доступа: для авторизир. Пользователей Основы информационной безопасности : учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В. Ю. Рогозин, И. Б. Галушкин, В. К. Новиков, С. Б. Вепрев. — Москва : ЮНИТИ-ДАНА, 2017. — 287 с. — ISBN 978-5-238-02857-6. — Текст : электронный // Электронный ресурс цифровой образовательной среды СПО PROFобразование : [сайт]. — URL: https://profspo.ru/books/72444 (дата обращения: 30.09.2022). — Режим доступа: для авторизир. пользователей Интернет-ресурсы: 1. http://www.consultant.ru/ – компьютерная справочная правовая система в Российской Федерации. 2. garant.ru – справочно-правовая система по законодательству Российской Федерации. 3.https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty – содержит нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. 4. http://bdu.fstec.ru/ – банк данных угроз безопасности информации содержит сведения об основных угрозах безопасности информации и уязвимостях, в первую очередь, характерных для государственных информационных систем и автоматизированных систем управления производственными и технологическими процессами критически важных объектов. 5. https://pd.rkn.gov.ru/ – портал персональных данных Роскомнадзора 6. https://www.itsec.ru/ -портал Информационная безопасность

3. ОРГАНИЗАЦИОННО-ПЕДАГОГИЧЕСКИЕ УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ

3.1. Требования к минимальному материально-техническому обеспечению

Материально-техническое обеспечение (далее – МТО) необходимо для проведения всех видов учебных занятий, промежуточной и итоговой аттестации, предусмотренных учебным планом по программе, и соответствует действующим санитарным и гигиеническим нормам и правилам.

Наименование специализированных аудиторий, кабинетов, лабораторий	**Вид занятий**	**Наименование оборудования, программного обеспечения**
Аудитория	Лекции	Персональный компьютер или ноутбук, с операционной системой не ниже Windows 7, объемом свободного пространства на жестком диске не менее 10 Гигабайт, объемом оперативной памяти не менее 4 Гигабайт; пакет офисных программ, например, Microsoft Office, Open Office или аналог; средство виртуализации VirtualBox. Мультимедийный проектор, экран, доска.
Лаборатория	Практические работы	Автоматизированное рабочее место студентов и преподавателя, инструкционно-технологические карты

3.2. Использование наглядных пособий и других учебных материалов при реализации программы

1. Мультимедийные презентации к лекционным и практическим занятиям.

2. Федеральная нормативно-правовая документация (приказы, положения, инструктивные письма, стандарты).

3. Локальная нормативно-правовая документация (положения, рабочие учебные планы, рабочие программы).

4. Диски с учебными видеокурсами.

3.3. Условия для функционирования электронной информационно-образовательной среды (при реализации программ с использованием дистанционных образовательных технологий)

Электронные информационные ресурсы	Вид занятий	Наименование оборудования, программного обеспечения
Система дистанционного обучения ОГАПОУ «Алексеевский колледж» http://moodle.alcollege.ru/ IPR BOOKS - http://www.iprbookshop.ru/78574.html	Лекционное, практическое	Автоматизированное рабочее место студентов

3.4. Кадровое обеспечение образовательного процесса. Требования к квалификации педагогических кадров

К реализации программы привлекается лица, имеющие высшее образование, направление которого соответствует профилю программы, опыт решения практических задач по тематике программы.

4. ОЦЕНКА КАЧЕСТВА ОСВОЕНИЯ ПРОГРАММЫ

Оценка качества освоения программы осуществляется в форме промежуточной и итоговой аттестации обучающихся.

Формой проведения промежуточной аттестации слушателей являются зачет и (или) дифференцированный зачет по завершению каждого модуля.

Оценка качества освоения программы осуществляется итоговой аттестационной комиссией в виде квалификационного экзамена.

Квалификационный экзамен включает в себя практическую квалификационную работу и проверку теоретических знаний в пределах квалификационных требований, указанных в профессиональном стандарте.

Задания для промежуточной аттестации:

Тест №1

Вопрос 1:Кто является основным ответственным за определение уровня классификации информации?

Варианты ответа:

а) Руководитель среднего звена

б) Высшее руководство

в) Владелец

г) Пользователь

Вопрос 2:Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

Варианты ответа:

а) Сотрудники

б) Хакеры

в) Атакующие

г) Контрагенты (лица, работающие по договору)

Вопрос 3:Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

Варианты ответа:

а) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

б) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

в) Улучшить контроль за безопасностью этой информации

г) Снизить уровень классификации этой информации

Вопрос 4:Что самое главное должно продумать руководство при классификации данных?

Варианты ответа:

а) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным

б) Необходимый уровень доступности, целостности и конфиденциальности

в) Оценить уровень риска и отменить контрмеры

г) Управление доступом, которое должно защищать данные

Вопрос5:Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

Варианты ответа:

а) Владельцы данных

б) Пользователи

в) Администраторы

г) Руководство

Вопрос 6:Что такое процедура?

Варианты ответа:

а) Правила использования программного и аппаратного обеспечения в компании

б) Пошаговая инструкция по выполнению задачи

в) Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

г) Обязательные действия

Вопрос 7:Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

Варианты ответа:

а) Поддержка высшего руководства

б) Эффективные защитные меры и методы их внедрения

в) Актуальные и адекватные политики и процедуры безопасности

г) Проведение тренингов по безопасности для всех сотрудников

Вопрос 8:Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Варианты ответа:
а) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
б) Когда риски не могут быть приняты во внимание по политическим соображениям
в) Когда необходимые защитные меры слишком сложны
г) Когда стоимость контрмер превышает ценность актива и потенциальные потери
Вопрос 9:Что такое политики безопасности?
Варианты ответа:
а) Пошаговые инструкции по выполнению задач безопасности
б) Общие руководящие требования по достижению определенного уровня безопасности
в) Широкие, высокоуровневые заявления руководства
г) Детализированные документы по обработке инцидентов безопасности
Вопрос 10: Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Варианты ответа:
а) Анализ рисков
б) Анализ затрат / выгоды
в) Результаты ALE
г) Выявление уязвимостей и угроз, являющихся причиной риска
Вопрос 11: Что лучше всего описывает цель расчета ALE?
Варианты ответа:
а) Количественно оценить уровень безопасности среды
б) Оценить возможные потери для каждой контрмеры
в) Количественно оценить затраты / выгоды
г) Оценить потенциальные потери от угрозы в год
Вопрос 12: Тактическое планирование – это:
Варианты ответа:
а) Среднесрочное планирование
б) Долгосрочное планирование
в) Ежедневное планирование
г) Планирование на 6 месяцев
Вопрос 13: Что является определением воздействия (exposure) на безопасность?
Варианты ответа:
а) Нечто, приводящее к ущербу от угрозы
б) Любая потенциальная опасность для информации или систем
в) Любой недостаток или отсутствие информационной безопасности
г) Потенциальные потери от угрозы
Вопрос 14: Эффективная программа безопасности требует сбалансированного применения:
Варианты ответа:
а) Технических и нетехнических методов
б) Контрмер и защитных механизмов
в) Физической безопасности и технических средств защиты
г) Процедур безопасности и шифрования
Вопрос 15: Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
Варианты ответа:
а) Внедрение управления механизмами безопасности
б) Классификацию данных после внедрения механизмов безопасности
в) Уровень доверия, обеспечиваемый механизмом безопасности

г) Соотношение затрат / выгод
Вопрос 16: Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
Варианты ответа:
а) Только военные имеют настоящую безопасность
б) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
в) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
г) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности
Вопрос 17:Как рассчитать остаточный риск?
Варианты ответа:
а) Угрозы х Риски х Ценность актива
б) (Угрозы х Ценность актива х Уязвимости) х Риски
в) SLE х Частоту = ALE
г) (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля
Вопрос 18: Что из перечисленного не является целью проведения анализа рисков?
Варианты ответа:
а) Делегирование полномочий
б) Количественная оценка воздействия потенциальных угроз
в) Выявление рисков
г) Определение баланса между воздействием риска и стоимостью необходимых контрмер
Вопрос 19: Что представляет собой стандарт ISO/IEC 27799?
Варианты ответа:
а) Стандарт по защите персональных данных о здоровье
б) Новая версия BS 17799
в) Определения для новой серии ISO 27000
г) Новая версия NIST 800-60
Вопрос 20: Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
Варианты ответа:
а) Безопасная OECD
б) ISOIEC
в) OECD
г) CPTED

Тест №2.

1. СВЕДЕНИЯ (СООБЩЕНИЯ, ДАННЫЕ) НЕЗАВИСИМО ОТ ФОРМЫ ИХ ПРЕДСТАВЛЕНИЯ:
1. Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации
2. ПРОЦЕССЫ, МЕТОДЫ ПОИСКА, СБОРА, ХРАНЕНИЯ, ОБРАБОТКИ, ПРЕДОСТАВЛЕНИЯ, РАСПРОСТРАНЕНИЯ ИНФОРМАЦИИ И СПОСОБЫ ОСУЩЕСТВЛЕНИЯ ТАКИХ ПРОЦЕССОВ И МЕТОДОВ:
1. Информация
2. Информационные технологии
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Обладатель информации

3. ЛИЦО, САМОСТОЯТЕЛЬНО СОЗДАВШЕЕ ИНФОРМАЦИЮ ЛИБО ПОЛУЧИВШЕЕ НА ОСНОВАНИИ ЗАКОНА ИЛИ ДОГОВОРА ПРАВО РАЗРЕШАТЬ ИЛИ ОГРАНИЧИВАТЬ ДОСТУП К ИНФОРМАЦИИ:
1. Источник информации
2. Потребитель информации
3. Уничтожитель информации
4. Носитель информации
5. Обладатель информации
4. ТЕХНОЛОГИЧЕСКАЯ СИСТЕМА, ПРЕДНАЗНАЧЕННАЯ ДЛЯ ПЕРЕДАЧИ ПО ЛИНИЯМ СВЯЗИ ИНФОРМАЦИИ, ДОСТУП К КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ИСПОЛЬЗОВАНИЕМ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ ЭТО:
1. База данных
2. Информационная технология
3. Информационная система
4. Информационно-телекоммуникационная сеть
5. Медицинская информационная система
5. ОБЯЗАТЕЛЬНОЕ ДЛЯ ВЫПОЛНЕНИЯ ЛИЦОМ, ПОЛУЧИВШИМ ДОСТУП К ОПРЕДЕЛЕННОЙ ИНФОРМАЦИИ, ТРЕБОВАНИЕ НЕ ПЕРЕДАВАТЬ ТАКУЮ ИНФОРМАЦИЮ ТРЕТЬИМ ЛИЦАМ БЕЗ СОГЛАСИЯ ЕЕ ОБЛАДАТЕЛЯ ЭТО:
1. Электронное сообщение
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации
6. ДЕЙСТВИЯ, НАПРАВЛЕННЫЕ НА ПОЛУЧЕНИЕ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННЫМ КРУГОМ ЛИЦ ИЛИ ПЕРЕДАЧУ ИНФОРМАЦИИ НЕОПРЕДЕЛЕННОМУ КРУГУ ЛИЦ ЭТО:
1. Уничтожение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации
7. ВОЗМОЖНОСТЬ ПОЛУЧЕНИЯ ИНФОРМАЦИИ И ЕЕ ИСПОЛЬЗОВАНИЯ ЭТО:
1. Сохранение информации
2. Распространение информации
3. Предоставление информации
4. Конфиденциальность информации
5. Доступ к информации
8. ИНФОРМАЦИЯ, ПЕРЕДАННАЯ ИЛИ ПОЛУЧЕННАЯ ПОЛЬЗОВАТЕЛЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ:
1. Электронное сообщение
2. Информационное сообщение
3. Текстовое сообщение
4. Визуальное сообщение
5. SMS-сообщение
9. ВСЕ КОМПОНЕНТЫ ИНФОРМАЦИОННОЙ СИСТЕМЫ ПРЕДПРИЯТИЯ, В КОТОРОМ НАКАПЛИВАЮТСЯ И ОБРАБАТЫВАЮТСЯ ПЕРСОНАЛЬНЫЕ ДАННЫЕ ЭТО:
1. Информационная система персональных данных
2. База данных
3. Централизованное хранилище данных
4. Система Статэкспресс

5. Сервер
10. К СВЕДЕНИЯМ КОНФИДЕНЦИАЛЬНОГО ХАРАКТЕРА, СОГЛАСНО УКАЗУ ПРЕЗИДЕНТА РФ ОТ 6 МАРТА 1997 Г., ОТНОСЯТСЯ:
1. Информация о распространении программ
2. Информация о лицензировании программного обеспечения
3. Информация, размещаемая в газетах, Интернете
4. Персональные данные
5. Личная тайна
11. ОТНОШЕНИЯ, СВЯЗАННЫЕ С ОБРАБОТКОЙ ПЕРСОНАЛЬНЫХ ДАННЫХ, РЕГУЛИРУЮТСЯ ЗАКОНОМ…
1. «Об информации, информационных технологиях»
2. «О защите информации»
3. Федеральным законом «О персональных данных»
4. Федеральным законом «О конфиденциальной информации»
5. «Об утверждении перечня сведений конфиденциального характера»
12. ДЕЙСТВИЯ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ (СОГЛАСНО ЗАКОНУ), ВКЛЮЧАЯ СБОР, СИСТЕМАТИЗАЦИЮ, НАКОПЛЕНИЕ, ХРАНЕНИЕ, ИСПОЛЬЗОВАНИЕ, РАСПРОСТРАНЕНИЕ И Т. Д ЭТО:
1. «Исправление персональных данных»
2. «Работа с персональными данными»
3. «Преобразование персональных данных»
4. «Обработка персональных данных»
5. «Изменение персональных данных»
13. ДЕЙСТВИЯ, В РЕЗУЛЬТАТЕ КОТОРЫХ НЕВОЗМОЖНО ОПРЕДЕЛИТЬ ПРИНАДЛЕЖНОСТЬ ПЕРСОНАЛЬНЫХ ДАННЫХ КОНКРЕТНОМУ СУБЪЕКТУ ПЕРСОНАЛЬНЫХ ДАННЫХ:
1. Выделение персональных данных
2. Обеспечение безопасности персональных данных
3. Деаутентификация
4. Деавторизация
5. Деперсонификация
14. ПО РЕЖИМУ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ В ИНФОРМАЦИОННОЙ СИСТЕМЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ ПОДРАЗДЕЛЯЮТСЯ НА:
1. Многопользовательские
2. Однопользовательские
3. Без разграничения прав доступа
4. С разграничением прав доступа
5. Системы, не имеющие подключений
15. ПРОЦЕСС СООБЩЕНИЯ СУБЪЕКТОМ СВОЕГО ИМЕНИ ИЛИ НОМЕРА, С ЦЕЛЬЮ ПОЛУЧЕНИЯ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ (ПРАВ ДОСТУПА) НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ:
1. Авторизация
2. Аутентификация
3. Обезличивание
4. Деперсонализация
5. Идентификация
16. ПРОЦЕДУРА ПРОВЕРКИ СООТВЕТСТВИЯ СУБЪЕКТА И ТОГО, ЗА КОГО ОН ПЫТАЕТСЯ СЕБЯ ВЫДАТЬ, С ПОМОЩЬЮ НЕКОЙ УНИКАЛЬНОЙ ИНФОРМАЦИИ:
1. Авторизация
2. Обезличивание
3. Деперсонализация

4. Аутентифика́ция
5. Идентификация
17. ПРОЦЕСС, А ТАКЖЕ РЕЗУЛЬТАТ ПРОЦЕССА ПРОВЕРКИ НЕКОТОРЫХ ОБЯЗАТЕЛЬНЫХ ПАРАМЕТРОВ ПОЛЬЗОВАТЕЛЯ И, ПРИ УСПЕШНОСТИ, ПРЕДОСТАВЛЕНИЕ ЕМУ ОПРЕДЕЛЁННЫХ ПОЛНОМОЧИЙ НА ВЫПОЛНЕНИЕ НЕКОТОРЫХ (РАЗРЕШЕННЫХ ЕМУ) ДЕЙСТВИЙ В СИСТЕМАХ С ОГРАНИЧЕННЫМ ДОСТУПОМ
1. Авториза́ция
2. Идентификация
3. Аутентификация
4. Обезличивание
5. Деперсонализация
18. ПРОСТЕЙШИМ СПОСОБОМ ИДЕНТИФИКАЦИИ В КОМПЬЮТЕРНОЙ СИСТЕМЕ ЯВЛЯЕТСЯ ВВОД ИДЕНТИФИКАТОРА ПОЛЬЗОВАТЕЛЯ, КОТОРЫЙ ИМЕЕТ СЛЕДУЮЩЕЕ НАЗВАНИЕ:
1. Токен
2. Password
3. Пароль
4. Login
5. Смарт-карта
19. ОСНОВНОЕ СРЕДСТВО, ОБЕСПЕЧИВАЮЩЕЕ КОНФИДЕНЦИАЛЬНОСТЬ ИНФОРМАЦИИ, ПОСЫЛАЕМОЙ ПО ОТКРЫТЫМ КАНАЛАМ ПЕРЕДАЧИ ДАННЫХ, В ТОМ ЧИСЛЕ – ПО СЕТИ ИНТЕРНЕТ:
1. Идентификация
2. Аутентификация
3. Авторизация
4. Экспертиза
5. Шифрование
20. ДЛЯ БЕЗОПАСНОЙ ПЕРЕДАЧИ ДАННЫХ ПО КАНАЛАМ ИНТЕРНЕТ ИСПОЛЬЗУЕТСЯ ТЕХНОЛОГИЯ:
1. WWW
2. DICOM
3. VPN
4. FTP
5. XML
21. КОМПЛЕКС АППАРАТНЫХ И/ИЛИ ПРОГРАММНЫХ СРЕДСТВ, ОСУЩЕСТВЛЯЮЩИЙ КОНТРОЛЬ И ФИЛЬТРАЦИЮ СЕТЕВОГО ТРАФИКА В СООТВЕТСТВИИ С ЗАДАННЫМИ ПРАВИЛАМИ И ЗАЩИЩАЮЩИЙ КОМПЬЮТЕРНЫЕ СЕТИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА:
1. Антивирус
2. Замок
3. Брандма́уэр
4. Криптография
5. Экспертная система
22. ЗА ПРАВОНАРУШЕНИЯ В СФЕРЕ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И ЗАЩИТЫ ИНФОРМАЦИИ ДАННЫЙ ВИД НАКАЗАНИЯ НА СЕГОДНЯШНИЙ ДЕНЬ НЕ ПРЕДУСМОТРЕН:
1. Дисциплинарные взыскания
2. Административный штраф
3. Уголовная ответственность
4. Лишение свободы
5. Смертная казнь

23. НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП К ИНФОРМАЦИИ ЭТО:
1. Доступ к информации, не связанный с выполнением функциональных обязанностей и не оформленный документально
2. Работа на чужом компьютере без разрешения его владельца
3. Вход на компьютер с использованием данных другого пользователя
4. Доступ к локально-информационной сети, связанный с выполнением функциональных обязанностей
5. Доступ к СУБД под запрещенным именем пользователя
24. «ПЕРСОНАЛЬНЫЕ ДАННЫЕ» ЭТО:
1. Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу
2. Фамилия, имя, отчество физического лица
3. Год, месяц, дата и место рождения, адрес физического лица
4. Адрес проживания физического лица
5. Сведения о семейном, социальном, имущественном положении человека, составляющие понятие «профессиональная тайна»
25. В ДАННОМ СЛУЧАЕ СОТРУДНИК УЧРЕЖДЕНИЯ МОЖЕТ БЫТЬ ПРИВЛЕЧЕН К ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:
1. Выход в Интернет без разрешения администратора
2. При установке компьютерных игр
3. В случаях установки нелицензионного ПО
4. В случае не выхода из информационной системы
5. В любом случае неправомочного использования конфиденциальной информации при условии письменного предупреждения сотрудника об ответственности
26. МОЖЕТ ЛИ СОТРУДНИК БЫТЬ ПРИВЛЕЧЕН К УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НАРУШЕНИЯ ПРАВИЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ:
1. Нет, только к административной ответственности
2. Нет, если это государственное предприятие
3. Да
4. Да, но только в случае, если действия сотрудника нанесли непоправимый вред
5. Да, но только в случае осознанных неправомочных действий сотрудника
27. ПРОЦЕДУРА, ПРОВЕРЯЮЩАЯ, ИМЕЕТ ЛИ ПОЛЬЗОВАТЕЛЬ С ПРЕДЪЯВЛЕННЫМ ИДЕНТИФИКАТОРОМ ПРАВО НА ДОСТУП К РЕСУРСУ ЭТО:
1. Идентификация
2. Аутентификация
3. Стратификация
4. Регистрация
5. Авторизация
28. НАИБОЛЕЕ ОПАСНЫМ ИСТОЧНИКОМ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ ЯВЛЯЮТСЯ:
1. Другие предприятия (конкуренты)
2. Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
3. Рядовые сотрудники предприятия
4. Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
5. Хакеры
29. ВЫБЕРИТЕ, МОЖНО ЛИ В СЛУЖЕБНЫХ ЦЕЛЯХ ИСПОЛЬЗОВАТЬ ЭЛЕКТРОННЫЙ АДРЕС (ПОЧТОВЫЙ ЯЩИК), ЗАРЕГИСТРИРОВАННЫЙ НА ОБЩЕДОСТУПНОМ ПОЧТОВОМ СЕРВЕРЕ, НАПРИМЕР НА MAIL.RU:

1. Нет, не при каких обстоятельствах
2. Нет, но для отправки срочных и особо важных писем можно
3. Можно, если по нему пользователь будет пересылать информацию, не содержащую сведений конфиденциального характера
4. Можно, если информацию предварительно заархивировать с помощью программы winrar с паролем
5. Можно, если других способов электронной передачи данных на предприятии или у пользователя в настоящий момент нет, а информацию нужно переслать срочно
30. ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТ В СООТВЕТСТВИИ С ЗАКОНАДЕЛЬСТВОМ РФ:
1. Информация составляющая государственную тайну
2. Информация составляющая коммерческую тайну
3. Персональная
4. Конфиденциальная информация
5. Документированная информация
31. ДЛЯ ТОГО ЧТОБЫ СНИЗИТЬ ВЕРОЯТНОСТЬ УТРАТЫ ИНФОРМАЦИИ НЕОБХОДИМО:
1. Регулярно производить антивирусную проверку компьютера
2. Регулярно выполнять проверку жестких дисков компьютера на наличие ошибок
3. Регулярно копировать информацию на внешние носители (сервер, компакт-диски, флэш-карты)
4. Защитить вход на компьютер к данным паролем
5. Проводить периодическое обслуживание ПК
31. ПАРОЛЬ ПОЛЬЗОВАТЕЛЯ ДОЛЖЕН
1. Содержать цифры и буквы, знаки препинания и быть сложным для угадывания
2. Содержать только цифры
3. Содержать только буквы
4. Иметь явную привязку к владельцу (его имя, дата рождения, номер телефона и т.п.)
5. Быть простым и легко запоминаться, например «123», «111», «qwerty» и т.д.
33. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЕСПЕЧИВАЕТ…
1. Блокирование информации
2. Искажение информации
3. Сохранность информации
4. Утрату информации
5. Подделку информации
34. ЗАКОН РОССИЙСКОЙ ФЕДЕРАЦИИ «О ГОСУДАРСТВЕННОЙ ТАЙНЕ» БЫЛ ПРИНЯТ В СЛЕДУЮЩЕМ ГОДУ:
1. 1982
2. 1985
3. 1988
4. 1993
5. 2005
36. ДОКУМЕНТИРОВАННОЙ ИНФОРМАЦИЕЙ, ДОСТУП К КОТОРОЙ ОГРАНИЧЕН В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РФ, НАЗЫВАЕТСЯ
1. Конфиденциальная
2. Персональная
3. Документированная
4. Информация составляющая государственную тайну
5. Информация составляющая коммерческую тайну
37. ИНФОРМАЦИЯ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЕ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОПИСАНА В:
1. 1 главе Уголовного кодекса

2. 5 главе Уголовного кодекса
3. 28 главе Уголовного кодекса
4. 100 главе Уголовного кодекса
5. 1000 главе Уголовного кодекса
38. В СТАТЬЕ 272 УГОЛОВНОГО КОДЕКСА ГОВОРИТСЯ…
1. О неправомерном доступе к компьютерной информации
2. О создании, исполнении и распространении вредоносных программ для ЭВМ
3. О нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети
4. О преступлениях в сфере компьютерной информации
5. Об ответственности за преступления в сфере компьютерной информации
39. НА РИСУНКЕ ИЗОБРАЖЕНО…
1. Настольная видеокамера
2. Оптическая мышь
3. Телефонная трубка
4. Электронный замок
5. Аппаратный модули доверенной загрузки «Аккорд - АМДЗ»
40. ФЕДЕРАЛЬНЫЙ ЗАКОН «ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ» НАПРАВЛЕН НА:
1. Регулирование взаимоотношений в информационной сфере совместно с гражданским кодексом РФ
2. Регулирование взаимоотношений в гражданском обществе РФ
3. Регулирование требований к работникам служб, работающих с информаций
4. Формирование необходимых норм и правил работы с информацией
5. Формирование необходимых норм и правил, связанных с защитой детей от информации
41. ХИЩЕНИЕ ИНФОРМАЦИИ – ЭТО…
1. Несанкционированное копирование информации
2. Утрата информации
3. Блокирование информации
4. Искажение информации
5. Продажа информации
42. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ПЕРВОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…
1. Государство
2. Коммерческая организация
3. Муниципальное учреждение
4. Любой гражданин
5. Группа лиц, имеющих общее дело
43. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ВТОРОЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…
1. Простые люди
2. Государство
3. Коммерческая организация
4. Муниципальное учреждение
5. Некоммерческая организация
44. ВЛАДЕЛЬЦЕМ ИНФОРМАЦИИ ТРЕТЬЕЙ КАТЕГОРИИ ЯВЛЯЕТСЯ…
1. Люди
2. Государство
3. Муниципальное учреждение
4. Учреждение
5. Некоммерческая организация
45. ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ ГОСУДАРСТВЕННУЮ ТАЙНУ, ВЛАДЕЮТ:
1. Государство
2. Только образовательные учреждения

3. Только президиум Верховного Совета РФ
4. Граждане Российской Федерации
5. Только министерство здравоохранения
46. ИНФОРМАЦИЕЙ, СОСТАВЛЯЮЩЕЙ КОММЕРЧЕСКУЮ ТАЙНУ, ВЛАДЕЮТ:
1. Государство
2. Различные учреждения
3. Государственная Дума
4. Граждане Российской Федерации
5. Медико-социальные организации
47. ПЕРСОНАЛЬНЫМИ ДАННЫМИ ВЛАДЕЮТ:
1. Государство
2. Различные учреждения
3. Государственная Дума
4. Жители Российской Федерации
5. Медико-социальные организации
48. ДОСТУП К ИНФОРМАЦИИ – ЭТО:
1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя
2. Действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц
3. Действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц
4. Информация, переданная или полученная пользователем информационно-телекоммуникационной сети
5. Возможность получения информации и ее использования
49. ДОКУМЕНТИРОВАННАЯ ИНФОРМАЦИЯ, ДОСТУП К КОТОРОЙ ОГРАНИЧИВАЕТСЯ В СООТВЕТСТВИИ С ЗАКОНОДАТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ ЭТО:
1. Конфиденциальная информация
2. Документы офера и договоров
3. Факс
4. Личный дневник
5. Законы РФ
50. ПЛАСТИКОВАЯ КАРТОЧКА, СОДЕРЖАЩАЯ ЧИП ДЛЯ КРИПТОГРАФИЧЕСКИХ ВЫЧИСЛЕНИЙ И ВСТРОЕННУЮ ЗАЩИЩЕННУЮ ПАМЯТЬ ДЛЯ ХРАНЕНИЯ ИНФОРМАЦИИ:
а. Токен
б. Password
в. Пароль
г. Login
д. Смарт-карта
51. УСТРОЙСТВО ДЛЯ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ, ПРЕДСТАВЛЯЮЩЕЕ СОБОЙ МОБИЛЬНОЕ ПЕРСОНАЛЬНОЕ УСТРОЙСТВО, НАПОМИНАЮЩИЕ МАЛЕНЬКИЙ ПЕЙДЖЕР, НЕ ПОДСОЕДИНЯЕМЫЕ К КОМПЬЮТЕРУ И ИМЕЮЩИЕ СОБСТВЕННЫЙ ИСТОЧНИК ПИТАНИЯ:
1. Токен
2. Автономный токен
3. USB-токен
4. Устройство iButton
5. Смарт-карта

52. ДОСТУП ПОЛЬЗОВАТЕЛЯ К ИНФОРМАЦИОННЫМ РЕСУРСАМ КОМПЬЮТЕРА И / ИЛИ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ ДОЛЖЕН РАЗРЕШАТЬСЯ ТОЛЬКО ПОСЛЕ:

1. Включения компьютера
2. Идентификации по логину и паролю
3. Запроса паспортных данных
4. Запроса доменного имени
5. Запроса ФИО

53. АППАРАТНЫЕ МОДУЛИ ДОВЕРЕННОЙ ЗАГРУЗКИ «АККОРД - АМДЗ» ПРЕДСТАВЛЯЮТ СОБОЙ…

1. Аппаратный контролер
2. Электронный замок
3. Система контроля
4. Сетевой адаптер
5. Копировальный аппарат

54. ЭЛЕКТРОННЫЕ ЗАМКИ «СОБОЛЬ» ПРЕДНАЗНАЧЕНЫ ДЛЯ …

1. Обеспечения доверенной загрузки компьютера и контроля целостности файлов в системах
2. Сканирования отпечатков пальцев
3. Проверки скорости и загрузки файлов
4. Общего контроля
5. Идентификации пользователя

55. Для защиты от злоумышленников необходимо использовать:

1. Системное программное обеспечение
2. Прикладное программное обеспечение
3. Антивирусные программы
4. Компьютерные игры
5. Музыку, видеофильмы

56. ФЕДЕРАЛЬНЫЙ ЗАКОН "ОБ ИНФОРМАЦИИ, ИНФОРМАТИЗАЦИИ И ЗАЩИТЕ ИНФОРМАЦИИ" ДАЕТ ОПРЕДЕЛЕНИЕ ИНФОРМАЦИИ:

1. Текст книги или письма
2. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления
3. Сведения о явлениях и процессах
4. Факты и идеи в формализованном виде
5. Шифрованный текст, текст на неизвестном языке

57. ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЕСТЬ ОБЕСПЕЧЕНИЕ…

1. Независимости информации
2. Изменения информации
3. Копирования информации
4. Сохранности информации
5. Преобразования информации

Критерии оценки:

Оценка	"2"	"3"	"4"	"5"
Отношение полученного количества баллов к максимально возможному (в процентах)	0% - 40%	41% - 60%	61% - 80%	81% -100%

Перечень вопросов теоретической части квалификационного экзамена

1. Прогресс информационных технологий и необходимость обеспечения информационной безопасности.
2. Основные понятия информационной безопасности.
3. Структура понятия информационная безопасность.
4. Система защиты информации и ее структура.
5. Профессиональные тайны, их виды. Объекты коммерческой тайны на предприятии.
6. Персональные данные и их защита.
7. Информационные угрозы, их виды и причины возникновения.
8. Информационные угрозы для государства.
9. Информационные угрозы для компании.
10. Информационные угрозы для личности (физического лица).
11. Действия и события, нарушающие информационную безопасность.
12. Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.
13. Способы воздействия информационных угроз на объекты.
14. Внешние и внутренние субъекты информационных угроз.
15. Компьютерные преступления и их классификация.
16. Исторические аспекты компьютерных преступлений и современность.
17. Вредоносные программы, их виды
18. История компьютерных вирусов и современность.
19. Государственное регулирование информационной безопасности.
20. Деятельность международных организаций в сфере информационной безопасности.
21. Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.

22. Уголовно-правовой контроль над компьютерной преступностью в России.

23. Федеральные законы по ИБ в РФ.

24. Политика безопасности и ее принципы.

25. Фрагментарный и системный подход к защите информации.

26. Методы и средства защиты информации.

27. Организационное обеспечение ИБ.

28. Защита информации в Интернете.

29. Электронная почта и ее защита.

30. Защита от компьютерных вирусов.

31. «Больные» мобильники и их «лечение».

32. Популярные антивирусные программы и их классификация.

33. Организация системы защиты информации экономических объектов.

34. Криптографические методы защиты информации.

35. Этапы построения системы защиты информации.

36. Электронная коммерция и ее защита.

37. Менеджмент и аудит информационной безопасности на уровне предприятия.

38. Информационная безопасность предпринимательской деятельности.

39. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов.

Критерии оценки

Устный опрос является одним из основных способов учета знаний обучающихся. Развернутый ответ должен представлять собой связное, логически последовательное сообщение на определенную тему, показывать его умение применять определения, правила в конкретных случаях.

При оценке ответа надо руководствоваться следующими критериями:

1) полнота и правильность ответа;

2) степень осознанности, понимания изученного;

3) языковое оформление ответа.

Оценка «5» ставится, если полно излагает изученный материал, дает правильные определения языковых понятий; может обосновать свои суждения.

Оценка «4» ставится, если обучающийся дает ответ, удовлетворяющий тем же требованиям, что и для оценки «5», но допускает 1—2 ошибки, которые сам же исправляет, и 1—2 недочета в последовательности и языковом оформлении излагаемого.

Оценка «3» ставится, если ученик демонстрирует знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры, излагает материал непоследовательно и допускает ошибки.

Оценка «2» ставится, если ученик обнаруживает незнание большей части соответствующего раздела изучаемого материала, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Перечень практических заданий квалификационного экзамена

Задание 1. Защита информации. Безопасность информации (данных). Информационная безопасность. Архитектурная безопасность.

Задание 2. Законодательство об информационных правоотношениях. Уровни правового обеспечения информационной безопасности информации и информационной безопасности предприятия.

Задание 3. Случайные угрозы. Преднамеренные угрозы. Разновидность угроз информационным процессам.

Задание 4. Обзор организационных методов защиты информационных процессов в компьютерных системах. Контроль доступа к аппаратуре.

Разграничение и контроль доступа. Разделение привилегий на доступ. Идентификация и установление подлинности. Аутентификация.

Задание 5. Концептуальные основы построения защиты информационных процессов от несанкционированного доступа в компьютерных системах. Модель поведения потенциального нарушителя.

Задание 6. Модель защиты информационного процесса. Оценка эффективности автоматических средств управления защитой информационных процессов в компьютерных системах.

Задание 7. Уровни защиты данных в сети. Распределение средств защиты в модели взаимосвязи открытых систем.

Задание 8. Классификация систем защиты программного обеспечения и технические средства программно-аппаратной защиты информационных процессов. Достоинства и недостатки основных систем защиты. Системы защиты от несанкционированного копирования.

Задание 9. Специфика возникновения угроз и механизмы защиты от угроз в открытых сетях. Механизмы защиты операционных систем.

Задание 10. Система безопасности ОС WINDOWS. Защита от информационных инфекций. Классификация компьютерных вирусов.

Задание 10. Программно - аппаратные методы защиты информационных процессов. Защита технических средств от несанкционированного доступа.

Критерии оценок обучающихся практических заданий

Оценка «5»:

- работа выполнена полностью, правильно; сделаны правильные наблюдения и выводы;

- практические приемы обработки деталей и узлов, изделия осуществлены правильно, с учетом техники безопасности и правил работы с оборудованием;

- проявлены организационно – трудовые умения (поддерживается чистота рабочего места и порядок на рабочем месте).

Оценка «4»:

- работа выполнена правильно, сделаны правильные наблюдения и выводы, при этом практические приемы обработки деталей и узлов, изделия осуществлены не полностью или допущены несущественные ошибки в работе с оборудованием.

Оценка «3»:

- работа выполнена правильно не менее чем наполовину или допущена существенная ошибка в ходе осуществления практических приемов обработки деталей и узлов, изделия, в объяснении, в оформлении работы, в соблюдении правил техники безопасности при работе с оборудованием, которая исправляется по требованию.

Оценка «2»:

- допущены две (или более) существенные ошибки в ходе осуществления практических приемов обработки деталей и узлов, изделия, в объяснении, в оформлении работы, в соблюдении правил техники безопасности при работе с оборудованием, которые обучающийся не может исправить по требованию;

- работа не выполнена, у обучающегося отсутствуют практические умения.

Результаты (освоенные профессиональные компетенции)	**Основные показатели оценки результата**	**Формы и методы контроля и оценки**
ПК 1.1. Производить установку и настройку компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Демонстрировать умения установки и настройки компонентов автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен

ПК 1.2. Администрировать программные и программно-аппаратные компоненты автоматизированной (информационной) системы в защищенном исполнении.	Проявление умения и практического опыта администрирования программных и программно-аппаратных компонентов автоматизированной (информационной) системы в защищенном исполнении	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен
ПК 1.3. Обеспечивать бесперебойную работу автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации.	Проведение перечня работ по обеспечению бесперебойной работы автоматизированных (информационных) систем в защищенном исполнении в соответствии с требованиями эксплуатационной документации	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен
ПК 1.4. Осуществлять проверку технического состояния, техническое обслуживание и текущий ремонт, устранять отказы и восстанавливать работоспособность автоматизированных (информационных) систем в защищенном исполнении.	Проявлять знания и умения в проверке технического состояния, проведении текущего ремонта и технического обслуживания, в устранении отказов и восстановлении работоспособности автоматизированных (информационных) систем в защищенном исполнении	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен
ПК 2.1. Осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации.	Организовывать и проводить анализ, настройку и установку программно-аппаратных средств защиты информации	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен
ПК 2.2. Обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами.	Организация процесса защиты информации в автоматизированных системах с учетом внутренних и внешних факторов	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен
ПК 2.3. Осуществлять тестирование функций	Организация тестирования функций программных и	Оценка в рамках текущего контроля и на практических

отдельных программных и программно-аппаратных средств защиты информации.	программно-аппаратных средств защиты информации	занятиях, выполнения индивидуальных заданий, тестирования, экзамен
ПК 2.4. Осуществлять обработку, хранение и передачу информации ограниченного доступа.	Организация обработки, хранения и передачи информации ограниченного доступа	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен
ПК 2.5. Уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств.		Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен
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.	Организация регистрации основных событий в автоматизированных системах	Оценка в рамках текущего контроля и на практических занятиях, выполнения индивидуальных заданий, тестирования, экзамен

5. РУКОВОДИТЕЛЬ И СОСТАВИТЕЛИ ПРОГРАММЫ

Автор(ы)/составители:

Жук Наталья Михайловна, преподаватель ОГАПОУ «Алексеевский колледж»