МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное
образовательное учреждение высшего образования
«Национальный исследовательский Нижегородский государственный университет
им. Н.И. Лобачевского»

Институт экономики и предпринимательства

УТВЕРЖДЕНО
решением президиума ученого совета ННГУ
протокол от «14» декабря 2021 г. № 4

Рабочая программа дисциплины

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Уровень высшего образования
бакалавриат

Направление подготовки
38.03.01 Экономика

Направленность образовательной программы
Цифровые системы учета, анализа и аудита

Форма обучения
очная, очно-заочная

Нижний Новгород

2022 год

1. Место дисциплины в структуре ООП

Дисциплина Б1.О.15 «Информационная безопасность» относится к обязательной части ООП направления подготовки 38.03.01 «Экономика»

2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	**Планируемые результаты обучения по дисциплине (модулю), в соответствии с индикатором достижения компетенции**		**Наименование оценочного средства**
	Индикатор достижения компетенции* (код, содержание индикатора)	**Результаты обучения по дисциплине****	
ПК-3. Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений	ПК 3.1. Формирует, анализирует и интерпретирует финансово-экономическую информацию	Знать: нормативные, организационные средства защиты информации при формировании отчетности, планов, проектов хозяйствующих субъектов Уметь: использовать современные средства и технологии защиты данных. Владеть: средствами сбора, обработки и анализа данных с применением систем информационной безопасности.	Задачи, тест, дискуссия
	ПК 3.2. Выявляет тенденции и использует результаты анализа информации для принятия управленческих решений	Знать: современные средства и возможности систем информационной безопасности при обработке отчетности в целях принятия управленческих решений Уметь: использовать средства информационных технологий при решении профессиональных задач. Владеть: навыками работы с современными системами информационной безопасности при принятии управленческих решений	Задачи, тест, дискуссия
ОПК-6 Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-6.1 Понимает принципы работы современных информационных технологий	Знать: основные методы, способы и средства преобразования информации Уметь: работать с компьютером как средством управления информацией Владеть: основными способами обнаружения информационных угроз и использования с антивирусных программ	Задачи, тест, дискуссия
	ОПК 6.2. Использует принципы работы современных информационных технологий для решения задач профессиональной деятельности	Знать: функции и задачи менеджмента и аудита систем информационной безопасности Уметь: выявлять информационные угрозы, выбирать методы и средства управления и аудита систем информационной безопасности Владеть: принципами менеджмента и аудита систем информационной безопасности	Задачи, тест, дискуссия

3. Структура и содержание дисциплины

3.1 Трудоемкость дисциплины

	очная форма обучения	очно-заочная форма обучения
Общая трудоемкость	**__4_ ЗЕТ**	**__4_ ЗЕТ**
Часов по учебному плану	**144**	**144**
в том числе		
аудиторные занятия (контактная работа): **- занятия лекционного типа** **- занятия семинарского типа** **(практические занятия)**	 **32** **32**	 **8** **8**
самостоятельная работа	**42**	**90**
КСР	**2**	**2**
Промежуточная аттестация – **Экзамен - 36**		

3.2. Содержание дисциплины

Наименование и краткое содержание разделов и тем дисциплины	**Всего (часы)**			в том числе												
				Контактная работа (работа во взаимодействии с преподавателем), часы из них											**Самостоятельная работа обучающегося, часы**		
				Занятия лекционного типа			**Занятия семинарского типа**			**Занятия лабораторного типа**			**Всего**				
	Очная	Очно-заочная	с	Очная	Очно-заочная		Очная	Очно-заочная	Заочная	Очная	Очно-заочная		Очная	Очно-заочная		Очная	Очно-заочная	с
Тема 1. Теоретические аспекты информационной безопасности экономических систем	18	17		5	1	5		1					10	2		8	15	
Тема2. Понятие информационных угроз и их виды	18	17		5	1	5		1					10	2		8	15	
Тема 3. Государствен-ное регулирование информационной безопасности	18	17		5	1	5		1					10	2		8	15	

Тема 4.Подходы, принципы, методы и средства обеспечения безопасности	14	19		3	2	3		2					6	4		8	15	
Тема 5. Организация системы защиты информации	22	19		7	2	7		2					14	4		8	15	
Тема 6. Менеджмент и аудит систем информационной безопасности	16	17		7	1	7		1					14	2		2	15	
текущий контроль	2	2											2	2				
Промежуточная аттестация - экзамен	36	36																
Итого	144	144		32	8	32		8					66	18		42	90	

Практические занятия (семинарские занятия) организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предполагает широкое использование в учебном процессе активных и интерактивных форм проведения занятий (компьютерных программ, деловых игр, разбор конкретных ситуаций) в сочетании с внеаудиторной работой с целью формирования и развития профессиональных навыков студентов. В рамках данного курса возможны встречи с представителями компаний различных форм собственности, государственных и муниципальных органов.

На проведение практических занятий (семинарских занятий) в форме практической подготовки отводится __4__ часа.

Практическая подготовка направлена на формирование и развитие:

- практических навыков в соответствии с профилем ОП: *аналитической деятельности и компетенции ПК-3*: Способен анализировать и интерпретировать данные отечественной и зарубежной финансовой, бухгалтерской и иной информации, выявлять тенденции изменения экономических и социально-экономических показателей и использовать полученные сведения для принятия управленческих решений.

Текущий контроль успеваемости реализуется в рамках занятий семинарского типа, групповых или индивидуальных консультаций.

4. Учебно-методическое обеспечение самостоятельной работы обучающихся

В ходе изучения дисциплины уделяется внимание как теоретическому усвоению понятий информационной безопасности, так и приобретению, развитию и закреплению практических навыков и умений по использованию специализированных информационных средств и технологий при организации ИБ экономических систем.

На лекциях раскрываются основные вопросы рассматриваемой темы, делаются акценты на наиболее важные, сложные и проблемные положения изучаемого материала, которые должны быть приняты студентами во внимание.

На практических занятиях, ориентированных на предметную область будущей профессиональной деятельности студентов, выборочно контролируется степень усвоения студентами основных теоретических положений. Рассматривается технология применения аппаратно-программных средств для организации ИБ. При решении практических заданий используются не только инструментальные средства информационных технологий бизнес-индустрии, но и методы и понятия дисциплин финансово-экономического блока.

После изучения каждой темы предусматривается выполнение студентами самостоятельной работы с проверкой как степени усвоения ими теоретических, знаний, так и объема и качества приобретенных практических навыков и умений.

В ходе самостоятельной работы, при подготовке к плановым занятиям, экзамену студенты анализируют поставленные преподавателем задачи и проблемы и с использованием учебно-методической литературы, информационных систем, комплексов и технологий, материалов, найденных в глобальной сети Интернет, находят пути их разрешения.

Для достижения поставленных целей преподавания дисциплины реализуются следующие средства, способы и организационные мероприятия:

- изучение теоретического материала дисциплины на лекции с использованием компьютерных технологий;
- самостоятельное изучение теоретического материала дисциплины с использованием Internet-ресурсов, информационных баз, методических разработок, специальной и научной литературы;
- закрепление теоретического материала при проведении практических занятий с использованием учебного и научного оборудования, выполнения проблемно-ориентированных, поисковых, творческих заданий.

Самостоятельная работа является наиболее деятельным и творческим процессом, который выполняет ряд дидактических функций: способствует формированию диалектического мышления, вырабатывает высокую культуру умственного труда, совершенствует способы организации познавательной деятельности, воспитывает ответственность, целеустремленность, систематичность и последовательность в работе студентов, развивает у них бережное отношение к своему времени, способность доводить до конца начатое дело.

Контрольные вопросы и задания для проведения текущего контроля и промежуточной аттестации по итогам освоения дисциплины приведены в п. 5.2.

Для обеспечения самостоятельной работы обучающихся используется электронные курсы «Информационная безопасность» (*https://e-learning.unn.ru/enrol/index.php?id=4715 и https://e-learning.unn.ru/enrol/index.php?id=4760*), созданные в системе электронного обучения ННГУ - https://e-learning.unn.ru/.

5. Фонд оценочных средств для промежуточной аттестации по дисциплине (модулю), включающий:

5.1. Описание шкал оценивания результатов обучения по дисциплине

Уровень сформированности компетенций (индикатора достижения компетенций)	**Шкала оценивания сформированности компетенций**						
	плохо	**неудовлетворительно**	**удовлетворительно**	**хорошо**	**очень хорошо**	**отлично**	**превосходно**
	не зачтено		**зачтено**				
Знания	Отсутствие знаний теоретического материала. Невозможность оценить полноту знаний вследствие	Уровень знаний ниже минимальных требований. Имели место грубые ошибки.	Минимально допустимый уровень знаний. Допущено много негрубых ошибки.	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько негрубых	Уровень знаний в объеме, соответствующем программе подготовки. Допущено несколько несущественны	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок.	Уровень знаний в объеме, превышающем программу подготовки.

	отказа обучающегося от ответа			ошибок	х ошибок		
Умения	Отсутствие минимальных умений . Невозможность оценить наличие умений вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы основные умения. Имели место грубые ошибки.	Продемонстрированы основные умения. Решены типовые задачи с негрубыми ошибками. Выполнены все задания но не в полном объеме.	Продемонстрированы все основные умения. Решены все основные задачи с негрубыми ошибками. Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения. Решены все основные задачи . Выполнены все задания, в полном объеме, но некоторые с недочетами.	Продемонстрированы все основные умения,решены все основные задачи с отдельными несущественным недочетами, выполнены все задания в полном объеме.	Продемонстрированы все основные умения,. Решены все основные задачи. Выполнены все задания, в полном объеме без недочетов
Навыки	Отсутствие владения материалом. Невозможность оценить наличие навыков вследствие отказа обучающегося от ответа	При решении стандартных задач не продемонстрированы базовые навыки. Имели место грубые ошибки.	Имеется минимальный набор навыков для решения стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач с некоторыми недочетами	Продемонстрированы базовые навыки при решении стандартных задач без ошибок и недочетов.	Продемонстрированы навыки при решении нестандартных задач без ошибок и недочетов.	Продемонстрирован творческий подход к решению нестандартных задач

Шкала оценки при промежуточной аттестации

Оценка		Уровень подготовки
	превосходно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «превосходно», продемонстрированы знания, умения, владения по соответствующим компетенциям на уровне, выше предусмотренного программой
зачтено	**отлично**	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «отлично», при этом хотя бы одна компетенция сформирована на уровне «отлично»
	очень хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «очень хорошо», при этом хотя бы одна компетенция сформирована на уровне « очень хорошо»
	хорошо	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «хорошо», при этом хотя бы одна компетенция сформирована на уровне «хорошо»
	удовлетворительно	Все компетенции (части компетенций), на формирование которых направлена дисциплина, сформированы на уровне не ниже «удовлетворительно», при этом хотя бы одна компетенция

		сформирована на уровне «удовлетворительно»
не зачтено	**неудовлетворительно**	Хотя бы одна компетенция сформирована на уровне «неудовлетворительно», ни одна из компетенций не сформирована на уровне «плохо»
	плохо	Хотя бы одна компетенция сформирована на уровне «плохо»

5.2. Типовые контрольные задания или иные материалы, необходимые для оценки результатов обучения.

5.2.1 Контрольные вопросы к экзамену по дисциплине «Информационная безопасность»

	Вопрос	Код компетенции
1.	Основные тенденции развития информатизации в экономике.	ОПК-6
2.	Основные понятия информационной безопасности в экономике.	ОПК-6
3.	Информационная безопасность в цифровой экономике.	ОПК-6
4.	Экономическая информация как товар и объект безопасности.	ОПК-6
5.	Система защиты информации и её структура.	ОПК-6
	Информационные угрозы, их виды и причины возникновения.	ОПК-6
	Информационные угрозы для государства.	ОПК-6
	Информационные угрозы для компании.	ОПК-6
	Информационные угрозы для личности (физического лица).	ОПК-6
	Действия и события, нарушающие информационную безопасность.	ОПК-6
	Личностно-профессиональные характеристики и действия сотрудников, способствующих реализации информационных угроз.	ОПК-6
	Способы воздействия информационных угроз на объекты.	ОПК-6
	Внешние и внутренние субъекты информационных угроз.	ОПК-6
	Компьютерные преступления и их классификация.	ОПК-6
	Исторические аспекты компьютерных преступлений и современность.	ОПК-6
	Субъекты и причины совершения компьютерных преступлений.	ОПК-6
	Вредоносные программы, их виды.	ОПК-6
	История компьютерных вирусов и современность.	ОПК-6
	Государственное регулирование информационной безопасности.	ОПК-6
	Деятельность международных организаций в сфере информационной безопасности.	ОПК-6
	Нормативно-правовые аспекты в области информационной безопасности в Российской Федерации.	ОПК-6
	Доктрина информационной безопасности России.	ОПК-6
	Уголовно-правовой контроль над компьютерной преступностью в России.	ОПК-6
	Федеральные законы по ИБ в РФ.	ОПК-6
	Политика безопасности и ее принципы.	ОПК-6
	Фрагментарный и системный подход к защите информации.	ОПК-6
	Методы и средства защиты информации.	ОПК-6
	Организационное обеспечение ИБ.	ОПК-6
	Организация конфиденциального делопроизводства.	ПК – 3
	Комплекс организационно-технических мероприятий по обеспечению защиты информации.	ПК – 3
	Инженерно-техническое обеспечение компьютерной безопасности.	ПК – 3
	Организационно-правовой статус службы безопасности.	ПК – 3
	Защита информации в Интернете.	ПК – 3
	Электронная почта и ее защита.	ПК – 3
	Защита от компьютерных вирусов.	ПК – 3
	«Больные» мобильники и их «лечение».	ПК – 3
	Популярные антивирусные программы и их классификация.	ПК – 3
	Организация системы защиты информации экономических объектов.	ПК – 3
	Криптографические методы защиты информации.	ПК – 3
	Этапы построения системы защиты информации.	ПК – 3
	Оценка эффективности инвестиций в информационную безопасность.	ПК – 3
	План обеспечения непрерывной работы и восстановления функционирования автоматизированной информационной системы.	ПК – 3
	Управление информационной безопасности на государственном уровне.	ПК – 3

Аудит ИБ автоматизированных банковских систем.	ПК – 3
Электронная коммерция и ее защита.	ПК – 3
Менеджмент и аудит информационной безопасности на уровне предприятия.	ПК-3
Информационная безопасность предпринимательской деятельности.	ПК-3
Обеспечение информационной безопасности должностных лиц.	ПК-3

5.2.2. Типовые задания для оценки сформированности компетенции _ОПК-6____

1. Определить место и роль информационной безопасности при использовании личного компьютера и мобильных устройств. Охарактеризовать последствия взлома ваших личных аккаунтов в соц. сетях, электронной почты.

1. Вы работаете бухгалтером-экономистом. Под Вашим логином и паролем со счета предприятия ушли большие суммы денег неизвестным контрагентам. Последствия, Ваша ответственность.

2. Вы работаете клиентским менеджером. С Вашего компьютера похищена клиентская база. Конкуренты предложили Вашим клиентам более привлекательные условия и цены. Последствия. Ваша ответственность.

3. Приведите примеры нарушения информационной безопасности из собственной практики. Охарактеризуйте последствия. Какие действия предпринимало руководство Вашей организации? Как в дальнейшем складывалась карьера виновных сотрудников?

Типовые задания для оценки сформированности компетенции _ПК-3___

1.Защита информации от сбоев оборудования и случайной потери

1. Ответьте на вопрос: «Что подразумевается под сбоем оборудования?», «Что означает случайная потеря информации?»

1. Определите методы защиты

1 периодическое архивирование программ и данных. Причем, под словом «архивирование» понимается как создание простой резервной копии, так и создание копии с предварительным сжатием (компрессией) информации. В последнем случае используются специальные программы-архиваторы (Arj, Rar, Zip и др.);

1 автоматическое резервирование файлов. Если об архивировании должен заботиться сам пользователь, то при использовании программ автоматического резервирования команда на сохранение любого файла автоматически дублируется и файл сохраняется на двух автономных носителях (например, на двух винчестерах). Выход из строя одного из них не приводит к потере информации. Резервирование файлов широко используется, в частности, в банковском деле.

2 периодическая проверка исправности оборудования (в частности - поверхности жесткого диска) при помощи специальных программ. Например: Disk Doctor, ScanDisk . Подобные программы позволяют обнаружить дефектные участки на поверхности диска и соответствующим образом их пометить, чтобы при записи информации эти участки были обойдены.

3 периодическая оптимизация (дефрагментация) диска для рационального размещения файлов на нем, ускорения работы и уменьшения его износа.

Определите методы защиты от случайной потери или искажения информации, *хранящейся в компьютере:*

1 автоматический запрос на подтверждение команды, приводящей к изменению содержимого какого-либо файла. Если вы хотите удалить файл или разместить новый файл под редакторы позволяют сделать документ доступным только для чтения или скрыть файл, сделав недоступным его имя в программах работы с файлами;

2 возможность отменить последние действия. Если вы редактируете документ, то можете пользоваться функцией отмены последнего действия или группы действий, имеющейся во всех современных редакторах. Если вы ошибочно удалили нужный файл, то специальные программы позволяют его восстановить, правда, только в том случае, когда вы ничего не успели записать поверх удаленного файла;

2 разграничение доступа пользователей к ресурсам файловой системы, строгому

разделению системного и пользовательского режимов работы вычислительной системы.

Ответьте на вопрос: «Что означает защита информации от кражи?»

Определите методы защиты информации.

Необходимые пояснения. По данным аналитиков, источник 80% угроз информационной безопасности компании - это ее собственный персонал. Сотрудники работают с документами составляющими коммерческую тайну, следовательно, они получают возможность нанести существенный урон предприятию передавая конфиденциальную информацию конкурентам, выкладывая в публичный доступ или предоставляя любым заинтересованным лицам. Причин для подобных действий может быть сколько угодно - конфликт с работодателем, внешние угрозы, шантаж, желание заработать и т.д. Возможностей тоже хватает - документы можно скопировать на usb-диск, послать по электронной почте или просто выложить в интернет.

Запретить доступ к документам, содержащим коммерческую тайну абсолютно всем сотрудникам нельзя - ведь кто-то же должен их создавать и обрабатывать. Но контролировать персонал имеющий доступ к секретной информации необходимо.

Системы Защиты Информации построенные на базе файерволов и антивирусов не могут защитить от хищений (краж) конфиденциальной информации предприятия, сотрудниками, имеющими в силу своих служебных обязанностей беспрепятственный доступ к секретным данным. Они просто для этого не предназначены.

В настоящее время можно выделить следующие способы защиты от кражи конфиденциальной информации сотрудниками:

1. Отключить дисководы, usb-порты, сеть - эффективность максимальная, затраты минимальны, но применить практически невозможно - через usb-порты часто подключают мышь с клавиатурой, сеть является основой ИТ-инфраструктуры предприятия и доступ в интернет в большинстве случаев нужен для работы. К тому же возможно, что сотруднику часто надо по работе переносить большие объемы информации (не вся же информация с которой он работает секретная), так что возможность подключать usb-диски желательно тоже оставить.

1. Передаваемую в сеть информацию фильтровать анализаторами трафика и блокировать передачу секретной. К сожалению, эти методы годятся только для фильтрации входящей информации - т.е. для блокировки вирусов и развлекательного например контента. Максимум чего можно достичь - это защита от непреднамеренных действий персонала, влекущих случайную утечку секретной информации. От преднамеренного хищения конфиденциальных данных подобное ПО не спасет, т.к. защиту можно обмануть например. К тому же остаются не подконтрольными съемные носители (в основном usb-диски , т.к. пишущими оптическими приводами рабочие места оснащаются не очень часто).

2. Разграничение доступа к портам ввода/вывода. Большинство подобных программ представляет собой просто графический интерфейс, являющийся надстройкой над стандартными защитными механизмами ОС Windows, который позволяет устанавливать права доступа к различным портам (например, usb) для любого пользователя. Это решение также не лишено серьезных недостатков:

во-первых - контроль не распространяется на информацию, передаваемую по сети; во-вторых - права статичны, т.е. невозможно разрешить пользователю копировать на usb-диск несекретную информацию и запретить копировать секретную.

3. Система Защиты Информации SecrecyKeeper Corporate - разрабатывалась с учетом недостатков первых трех способов. Основное назначение Системы Защиты Информации SecrecyKeeper Corporate - предотвращение несанкционированного распространения (краж и утечек) конфиденциальной информации.

SecrecyKeeper Corporate дает службе безопасности предприятия следующие возможности:

реализовать полномочный контроль доступа к сменным носителям информации, таким как дискеты, usb- флеш-диски и т.п.;

ограничить доступ к конфиденциальной информации сотрудников ИТ-подразделений;

разделять информацию, хранящуюся как на рабочих станциях сотрудников, так и на серверах по степени секретности;

присвоить каждому сотруднику предприятия персональный уровень доступа к конфиденциальной информации;

ограничить несанкционированное распространение конфиденциальной информации на основе степени секретности данных и уровней доступа сотрудников;

динамически регулировать права доступа сотрудников к устройствам переноса информации (дискеты, usb-диски, интернет) в зависимости от уровня доступа сотрудника и уровней секретности документов с которыми ведется работа;

предоставлять данные по работе с конфиденциальной информацией.

На любой файл можно установить метку конфиденциальности - гриф (общедоступная, служебная, секретная);

Гриф может быть установлен на информацию доступ к которой предоставляется по сети (удаленно), такую как например базы данных, корпоративные интернет-порталы и т.п.

Для сотрудников вводятся следующие уровни доступа (каждый из которых также может принимать значения - общедоступная, служебная, секретная):

уровень доступа к информации - определяет к информации с каким максимальным грифом может получить доступ сотрудник;

уровень доступа к сети - определяет информацию с каким максимальным грифом, сотрудник может передать в сеть;

уровень доступа к сменным носителям - определяет информацию с каким максимальным грифом, сотрудник может скопировать на сменный носитель.

5.2.3. Типовые практические задания для оценки сформированности компетенции__ОПК-6___

1. Как по отношению к информации Вашей организации ведут себя конкурирующие фирмы? Пытаются ли они заполучить важную информацию? Каким образом это происходит?
2. Сайт фирмы. Что допустимо на нем размещать? Уместно ли размещать образцы договоров? Выскажите Ваше мнение. Как сейчас в условиях кризиса размещать прайсы? С минимальной ценой от какой то суммы? Поясните Вашу позицию.
3. Некая фирма решила торговать тем же ассортиментом что и ваша фирма. Запрашивает прайс у поставщика, программисты полностью копируют ваш интернет-магазин, меняют только главную страницу сайта. Как это предупредить заранее? Опишите Ваши действия.
4. У Вас небольшая фирма. Вид деятельности придумайте сами. Как угрозы информационной безопасности вашей деятельности вы предполагаете? Как вы будете защищать информацию?
5. ИТ-специалист вашей фирмы. Как вы будете работать с ним? По договору? Возьмете его в штат? Какие обязанности вы для него предусмотрите с учетом требований информационной безопасности? Бюджет ограничен. На что вы планируете потратить деньги в первую очередь при сотрудничестве с ИТ-специалистом?
6. На какой платформе вы бы поручили разработать сайт компании? Обоснуйте решение.
0 Ответьте на вопрос: «Что такое компьютерный вирус?».

Назовите разновидности вирусов

Определите методы защиты от вирусов.

Необходимые пояснения. Компьютерным вирусом называется специально написанная программа, способная самостоятельно создавать свои копии и внедряться в другие программы, в системные области дисковой памяти компьютера, распространяться по каналам связи. Отличительной особенностью компьютерного вируса является маленький объем программного кода

Например, вирус может вставить себя в начало некоторой программы, так что каждый раз при выполнении этой программы первым будет активизироваться вирус. Во время выполнения вирус может производить намеренную порчу, которая сейчас же становится заметной, или просто искать другие программы, к которым он может присоединить свои копии. Если «заражённая» программа будет передана на другой компьютер через сеть или дискету, вирус начнёт заражать программы на

новой машине, как только будет запущена переданная программа. Таким способом вирус переходит от машины к машине. В некоторых случаях вирусы

потихоньку распространяются на другие программы и не проявляют себя, пока не произойдёт определённое событие, например, наступит заданная дата, начиная с которой они будут «разрушать» всё вокруг. Разновидностей компьютерных вирусов очень много.

По среде обитания вирусов.

Сетевые вирусы используют для своего распространения команды и протоколы телекоммуникационных сетей.

Файловые вирусы чаще всего Внедряются в исполняемые файлы, имеющие расширение .exe и сот, но могут внедряться и в файлы с компонентами операционных систем, драйверы внешних устройств, объектные файлы и библиотеки, в командные пакетные файлы. При запуске зараженных программ вирус на некоторое время получает управление и в этот момент производит запланированные деструктивные действия и внедрение в другие файлы программ.

Загрузочные вирусы внедряются в загрузочный сектор дискеты или в главную загрузочную запись жесткого диска. Такой вирус изменяет программу начальной загрузки операционной системы, запуская необходимые для нарушения конфиденциальности программы или подменяя, для этой же цели, системные файлы, в основном это относится к файлам, обеспечивающим доступ пользователей в систему.

Документные вирусы (макровирусы) заражают текстовые файлы редакторов или электронных таблиц, используя макросы, которые сопровождают такие документы. Вирус активизируется, когда документ загружается в соответствующее приложение.

По способу заражения среды обитания

Резидентные вирусы после завершения инфицированной программы остаются в оперативной памяти и продолжают свои деструктивные действия, заражая другие исполняемые программы, вплоть до выключения компьютера.

Нерезидентные вирусы запускаются вместе с зараженной программой и удаляются из памяти вместе с ней.

По алгоритмам функционирования

Паразитирующие вирусы — это вирусы изменяющие содержимое зараженных файлов. Они легко обнаруживаются и удаляются из файла, так как имеют всегда один и тот же внедряемый программный код.

Троянские кони — вирусы, маскируемые под полезные программы, которые очень хочется иметь на своем компьютере. Наряду с полезными функциями, соответствующими устанавливаемой программе, вирус может выполнять функции, нарушающие работу системы, или собирать информацию, обрабатываемую в ней.

Троянец — это разновидность вируса-червя, который может значительно повредить Ваш ПК, настолько серьезно, что может сломать Ваш компьютер за счет обширного повреждения, которое может быть необратимым. А так же троянцы стирают жесткий диск, посылают номера и пароли Ваших кредитных карточек по соответствующему адресу, используют компьютер в противоправных целях.

Троянский конь под названием Spy Sheriff заразил миллионы компьютеров по всему миру. Этот вирус группируется как malware, т. е. зловредное программное обеспечение. На компьютер и его систему он не оказывает влияние и не наносит ей вреда, но вынуждает появляться всяким непонятным всплывающим окнам. Почти все такие окна выглядят как сообщение от системы, сообщения, которые напрямую заявляют о том, что Вы обязаны установить то, или иное программное обеспечение. Большинство антивирусов не в состоянии обнаружить и удалить этот вирус. Этот вирус держит под контролем составляющие, которые управляют функцией восстановления системы, именно поэтому с помощью этой функции удалить вирус Spy Sheriff не удастся. Порой троянские программы могут находиться в архивах, которые внешне выглядят безопасными. Отдельные Трояны применяются преступниками и мошенниками для удалённого управления компьютером. Они также используются для взлома и хакерской атаки компьютерных систем.

Червь - это программа, очень похожая на вирус. Он способен к самовоспроизведению и может привести к негативным последствиям для Вашей системы. Однако для размножения червям не требуется заражать другие файлы.

Черви, в отличие от вирусов, просто копируют себя, повреждая файлы, но

репродуцирование может происходить очень быстро, сеть перенасыщается, что приводит к разрушению последней. Некоторые из наиболее печально известных червей включают (обычно посылаются через Интернет): I Love You, Navidad, Pretty Park, Happy99, ExploreZip. Для распространения, черви используют либо уязвимость на целевой системе, либо обман пользователя для их запуска. Червь попадает в компьютер через уязвимость в системе и использует функции перемещения файлов или информации в системе, что позволяет ему перемещаться и заражать компьютеры без посторонней помощи.

Боты

"Бот" - производное от слова "робот" и представляет собой автоматизированный процесс, который взаимодействует с другими сетевыми службами. Боты часто автоматизируют задачи и предоставления информации и услуг, которые могли бы производиться человеком. Типичным использованием ботов является сбор информации (например, сканер поисковой системы, ищущий новые сайты), а так же автоматизированное взаимодействие с человеком (например, автоответчик в аське или бот рассказывающий анекдоты).

Боты могут использоваться как в хороших, так и в плохих целях. Примером незаконных действий может служить бот-нет (сеть ботов). Вредоносный бот распространяет вредоносное ПО, которое заражает компьютеры и подключает их через бэкдоры к центральному серверу управления, который может управлять всей сетью взломанных устройств. Используя бот-нет злоумышленник может совершать DDOS-атаки на сайты или сервера конкурентов или по заказу. DDOS-атаки представляют собой одновременное огромное количеству бессмысленных запросов на сервер, исходящих от множества устройств (зараженных компьютеров), что приводит к перегрузке и зависанию сервера и невозможности нормальной работы и передачи информации (например, сайт перестает работать).

В дополнение к червеобразной способности самораспространяться, боты могут записывать нажатия клавиш, красть пароли, собирать финансовую информацию, совершать DDOS-атаки, рассылать спам. Боты имеют все преимущества червей, однако более универсальны и кроме того, объединены в сеть, которая позволяет контролировать зараженные компьютеры и совершать определенные действия по команде с контрольного центра. Создавая бэкдоры боты могут загружать на компьютер другие вредоносные программы, как вирусы или черви.

Боты в большинстве случаев стараются никак не проявлять себя для пользователя, поэтому опознать, что компьютер заражен бывает непросто.

Таким образом вредоносные боты являются наиболее опасными с точки зрения защиты информации, так как они не только сами распространяются и распространяют другое вредоносное ПО, но и способны совершать свои действия по команде из вне.

Эксплойты (Exploit)

Эксплойт является частью программного обеспечения, командами или методологией, которая нацелена на взлом конкретной уязвимости безопасности. Эксплойты не всегда обладают вредоносными намерениями. Они иногда используются только как способ демонстрации того, что существует уязвимость. Тем не менее, они являются общим компонентом вредоносных программ.

Бэкдоры (Backdoor)

Бэкдор (дословно "задняя дверь" или "черный ход") - это недокументированный путь доступа к системе, позволяющий злоумышленнику проникнуть в систему зараженного компьютера и управлять ей. Троян бэкдор (Trojan.Backdoor) при запуске как раз открывает тот самый "черный ход". Как правило злоумышленники используют бэкдоры для более удобного и постоянного доступа к взломанной системе. Через этот черный ход закачивается новое вредоносное ПО, вирусы и черви.

Вирусы-невидимки способны прятаться при попытках их обнаружения. Они перехватывают запрос антивирусной программы и либо временно удаляются из зараженного файла, либо подставляют вместо себя незараженные участки программы.

Мутирующие вирусы периодически изменяют свой программный код, что делает задачу обнаружения вируса очень сложной.

Репликаторы (вирусы-репликаторы), они же сетевые черви, проникают через компьютерные сети, они находят адреса компьютеров в сети и заражают их.

Создание, использование и распространение вредоносных программ для ЭВМ в РФ является преступлением.

Способы защиты от вирусов

Здесь эффективен комплекс мер, включающий в себя профилактические (использование антивирусных программ) и общие методы защиты.

Для защиты от вредоносных программ необходимо своевременно обновлять уже установленное ПО (обновлениями, выпущенными производителями), применять программы контроля работы с сетями — брандмауэры.

Брандмауэр (firewall), межсетевой экран — это средство, выполняющее фильтрацию входящей и исходящей информации на основе некоторой системы правил. Минимально необходимая функция (компонент) брандмауэра — пакетный фильтр, который анализирует пакеты и на основании данных об адресе отправителя и/или получателя, номера приложения-отправителя и/или получателя, статуса отправляемого пакета пропускает или отклоняет пакет. Такой брандмауэр способен сделать узел сети существенно менее «заметным», за счет того, что он перестает отвечать на не санкционированные пользователем попытки соединения. Брандмауэры, защищающие индивидуальных пользователей и небольшие сети, реализуются в виде как аппаратных средств, так и программных продуктов, устанавливаемых на ПК.

Для исключения проникновения вирусов через съемные носители необходимо ограничить число пользователей, которые могут записывать на жесткий диск файлы и запускать программы со съемных носителей. Обычно это право дается только администратору системы. В обязательном порядке при подключении съемного носителя следует проверять его специальной антивирусной программой.

Классификация антивирусных средств

Для обнаружения и удаления компьютерных вирусов разработано много различных программ, которые можно разделить на мониторы, детекторы, ревизоры, фильтры, доктора и вакцины.

Мониторы постоянно находятся в памяти компьютера и осуществляют автоматическую проверку всех используемых файлов в масштабе реального времени. Различаются три основных типа мониторов: файловые мониторы, мониторы для почтовых программ и мониторы для специальных приложений.

Детекторы (фаги) осуществляют поиск компьютерных вирусов в памяти и при обнаружении сообщают об этом пользователю.

Ревизоры выполняют значительно более сложные действия для обнаружения вирусов. Они запоминают исходное состояние программ, каталогов, системных областей и периодически сравнивают их с текущими значениями. При изменении контролируемых параметров ревизоры сообщают об этом пользователю.

Фильтры располагаются резидентно в оперативной памяти компьютера и "перехватывают" те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда.

Доктора являются самым распространенным типом антивирусных программ. Эти программы не только обнаруживают, но и удаляют вирусный код из файла — «лечат» программы. Доктора способны обнаружить и удалить только известные им вирусы, поэтому их необходимо периодически, обычно раз в месяц, обновлять.

Вакцины — это антивирусные программы, которые так модифицируют файл или диск, что он воспринимается программой-вирусом уже зараженным и поэтому вирус не внедряется.

Сканеры - антивирусные программы, выполняющие после запуска проверку заданной

области файловой структуры компьютера.

Современные антивирусные решения обладают всеми означенными механизмами и постоянно добавляют новые средства борьбы с вредоносными программами.

Популярные антивирусные средства

Среди наиболее популярных у российских пользователей антивирусных пакетов назовем программы: Norton Antivirus, Антивирус Касперского и Dr. Web.

Самый простой и эффективный способ обеспечить необходимую защиту мобильного телефона или КПК — это установить современную антивирусную программу, специально разработанную для защиты мобильных устройств от всех вирусных угроз. Антивирусы для мобильных устройств: смартфонов (ОС Symbian, Windows Mobile Smartphone), КПК и нетбуков.

Типовые практические задания для оценки сформированности компетенции__ПК-3

Задание

Установить антивирусное программное обеспечение на мобильное устройство и выполнить сканирование на вирусы

Разобрать практические ситуации

1. Связь основных понятий информационной безопасности

В издательство "Тезис" поступил звонок от провайдера. Предприятию отключили доступ к сети, потому что была зарегистрирована рассылка спама. Пришли большие счета, при сравнительно малом использовании ресурсов сети. В результате отключения Интернета были просрочены заказы, нарушена связь с несколькими клиентами, Оказалось, что менеджеры имеет несложный пароль, в основном даты рождения. У некоторых на мониторе приклеен стикер с паролем. Какие ошибки в информационном поведении сотрудников. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?

1. Основные уязвимости

Иногда изменяются содержательные данные, порой — служебная информация. Показательный случай нарушения целостности имел место в 1996 году. Служащая Oracle (личный секретарь вице-президента) возбудила судебный иск против президента корпорации, обвиняя его в незаконном увольнении после того, как она отвергла его ухаживания. В доказательство своей правоты женщина привела электронное письмо, якобы отправленное ее боссом президенту. Содержание письма для нас сейчас не важно; важно время отправки. Дело в том, что вице-президент предъявил, в свою очередь, файл с регистрационной информацией компании сотовой связи, из которого явствовало, что он (босс) в указанное время разговаривал по мобильному телефону, находясь за рулем автомобиля вдалеке от своего рабочего места. Таким образом, в суде состоялось противостояние "файл против файла". Очевидно, один из них был фальсифицирован или изменен, то есть была нарушена его целостность. Суд решил, что подделали электронное письмо (секретарь знала пароль своего босса, поскольку ей было поручено его регулярное изменение), и иск был отвергнут... Участники обсуждения делятся на защитников секретаря и защитников босса компании Oracle и доказывают правоту защищаемой стороны и возможность фальсификации доказательств противника.

2. История вирусов

Александр Квасов, начальник управления информационных технологий Нижегородского регионального центра-филиала ОАО АКБ «СОЮЗ»: — В конце 90-х много вирусов было настроено на остановку работоспособности компьютера — уничтожение информации в BIOS, и на жестких дисках. На себе я испытал поражение жесткого диска вирусом W95.CIH «Чернобыль». На офисных компьютерах стояла операционная система Windows 95, доступ в Интернет имел один компьютер, остальные были связаны с ним в локальной сети. 26 апреля 1999 года не загрузились все офисные компьютеры, информация

на дисках стала недоступной. Данные, к счастью, удалось восстановить, однако это было не так просто. Фирма понесла большие убытки.

Пометка для педагога: Напомним, что W95.CIH заражал исполняемые файлы и обладал крайне деструктивной функциональностью. Он полностью уничтожал содержимое жесткого диска и перезаписывал флэш-BIOS материнской платы, после чего заражённый компьютер вообще переставал загружаться. Наиболее .уязвимы для вируса компьютеры на базе операционных систем Windows 95, 98 и Me. В этом случае вирус ищет файлы с расширением .EXE и записывает свой код в неиспользуемые части этих файлов. Размер зараженных файлов при этом практически не увеличивается, и у пользователя не возникает никаких подозрений.

Участникам обсуждения проблемы предлагается представить себя на месте сотрудников ОАО АКБ «СОЮЗ», предложить варианты обнаружения заражения, проверки, профилактики, защиты данных.

3. Классификация вирусов

У журналиста-фрилансера возникли проблемы с программным обеспечением:

1. Большинство программ перестают работать и "вылетают" с критической ошибкой

1. Загрузка в безопасном режиме невозможна

2. Сайты kaspersky.ru, drweb.ru, viruslist.ru и пр. не загружаются

3. Значительно снизилась производительность компьютера. Он решил, что это - результат деятельности вируса.

Участникам обсуждения предлагается по симптомам определить, что за вирус, как его лечить

4. метка для педагога: Вирус, который Kaspersky определяет как VIRUS.WIN32.Sality.z, а Dr. Web - win32.sector.5, win32.sector.7 (подробное описание). Даже у опытных пользователей его уничтожение вызывает трудности.

Пример решения:

1. Отключаем сеть. Т.е. отключаем ADSLm Dial-up, LAN - любые сетевые подключения. Просто выдергиваем кабель.

1. Идем к неинфицированному компьютеру, т.к. на инфицированном не удастся получить доступ к сайту, и скачиваем Dr. Web CureIt!. Это бесплатное приложение, которое может работать даже без установки. Скачанное приложение по возможности записываем на CD/DVD или флешку с защитой - дабы вирус не мог испортить программу. Если испортит - вместо приветственного окошка вы увидите окно стандартного распаковщика WinRAR SFX.

2. Чиним реестр с помощью установки ключа. Соглашаемся с внесением изменений в реестр.

3. Загружаемся в безопасном режиме, удерживая длительное время сразу после включения компьютера клавишу F8. Должно появиться меню с выбором вариантов загрузки. Нам нужен "Безопасный режим".

4. Лечим компьютер от вирусов. Для этого вставляем диск с записанным Dr.Web CureIt! и проводим полную проверку компьютера.

5. Перезагружаемся в обычном режиме.

6. Вновь проводим полную проверку.

7. Устанавливаем нормальный антивирус со свежими базами.

5. Медиа вирусы

Студент факультета информатики был удивлен, заметив, что во время прослушивания определенного аудиофайла, активируется запуск браузера Internet Explorer, который переходит на страницу Интернета, где пользователю предлагается скачать и установить некий файл, выдаваемый за кодек со странным названием, расширением. Студент несколько раз отвергал установку. Студент описал происходящее на форуме сайта Virusov.net. Что узнал студент? Какой это вирус? Что он делает? Чем опасен, к чему приводит?

Пометка для педагога: Эксперты "Лаборатории Касперского" отмечают вирус GetCodec.d. По их мнению, это уникальный пример червя, заражающего аудиофайлы.

Напомним, что "червь", получивший название Worm.Win32.GetCodec.a, конвертирует трЗ-файлы в формат WMA (при этом сохраняя расширение mp3) и добавляет в них маркер, содержащий в себе ссылку на зараженную web-страницу. Активация маркера осуществляется автоматически во время прослушивания файла и приводит к запуску браузера Internet Explorer, который переходит на инфицированную страницу, где пользователю предлагается скачать и установить некий файл, выдаваемый за кодек. Если пользователь соглашается на установку, то на его компьютер загружается троянская программа Trojan-Proxy. Win32.Agent.arp, с помощью которой злоумышленник может получить контроль над атакованным ПК.

5. Почтовые вирусы

Анатолию пришло письмо с темой: "Лучшие рефераты" тело письма пустое, почтовое вложение - иконки HTML-документа Internet Explorer. Позднее Анатолий заметил на дисках новые файлы C:\ADMIN.DLL, D:\ADMIN.DLL, E:\ADMIN.DLL, а так же существование файла README.EML. Неожиданное наличие открытых общих сетевых ресурсов, несколько раз случалась перегрузка сети. Какой это вирус? Что он делает? Чем опасен, к чему приводит? Как его лечить?

Разобрать практические ситуации.

1. Компьютерная неграмотность персонала

В понедельник утром в фирму "Омега" поступил звонок от провайдера. Фирме отключили доступ к сети, потому что в период с 3.00 до 5.00 с адреса компьютера секретаря была совершена рассылка 1500 писем. Секретарь фирмы - Яна, имеет несложный пароль, состоящий из цифр, по совету системного администратора часто меняет его, но не придумывая новый, а переставляю цифры в старом, для запоминания клеит стикеры с паролем на монитор. Какие ошибки в информационном поведении сотрудницы. Как действовать в данной ситуации. Как избежать подобных ситуаций позднее?

1. Вы купили готовый бизнес - автомойка + шиномонтаж. Выполните аудит информационной безопасности предприятия. Проверьте наличие защиты компьютеров, хранение клиентской базы, доступ к АСУ, уровни доступа пользователей. Проверьте отключен ли доступ к АСУ у уволившихся сотрудников. Продолжите дальше список ваших действий.

2. Вы поступили на должность директора кафе. Проведите аудит информационной безопасности. Дайте рекомендации собственнику бизнеса.

3. Ответьте на вопрос «Что такое несанкционированный доступ?». Определите методы защиты.

4. Есть множество программ, помогающих защитить информацию на вашем компьютере. Ознакомьтесь и установите их.

Программный продукт SysUtils Device Manager Enterprise Edition обеспечивает разграничение доступа к устройствам хранения данных, использующим съемные носители информации, таким как дискетные дисководы, компакт-дисководы и накопители на флэш-памяти.

CD-DVD Lock - программа дает возможность запретить доступ на чтение или на запись съемных дисков - CD, DVD,USB, дискет, а также на определенные разделы жестких дисков. Можно ограничить доступ двумя путями: скрыть ваши устройства от возможности просмотра или закрыть к ним доступ.

TimeBoss - программа предназначена для управления временем работы пользователей, зарегистрированных в системе Windows. Позволяет ограничивать время, запрещать запуск отдельных указанных программ или программ, расположенных в определенных папках или дисках. Ведет журнал учета работы пользователей.

Lock 2.0 - предназначена для блокирования запуска приложений, графических и текстовых файлов. Lock не позволяет также перемещать, копировать и прикреплять к отправляемым по e- mail письмам указанные файлы. Что может существенно ограничить

доступ к Вашей информации посторонним лицам.

Критерии оценки задания

Превосходно	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, обучающийся отвечает четко и последовательно, показывает глубокое знание основного и дополнительного материала.
Отлично	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, обучающийся отвечает четко и последовательно, показывает глубокое знание основного материала
Очень хорошо	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, обучающийся отвечает четко и последовательно, показывает глубокое знание материала, допущено не более 2 неточностей непринципиального характера
Хорошо	Задание выполнено в полном объеме (все поставленные задачи решены), ответ логичен и обоснован, допущены неточности непринципиального характера, но обучающийся показывает систему знаний по теме своими ответами на поставленные вопросы
У довлетворительно	Задание выполнено не в полном объеме (решено более 50% поставленных задач), но обучающийся допускает ошибки, нарушена последовательность ответа, но в целом раскрывает содержание основного материала
Неудовлетворительно	Задание выполнено не в полном объеме (решено менее 50% поставленных задач), обучающийся дает неверную информацию при ответе на поставленные задачи, допускает грубые ошибки при толковании материала, демонстрирует незнание основных терминов и понятий.
Плохо	Задание не выполнено, обучающийся демонстрирует полное незнание материала

5.2.4. Темы для проведения дискуссий (ОПК-6, ПК-3)

1. Перечислите основополагающие документы по информационной безопасности.

2. Понятие государственной тайны.

3. Что понимается под средствами защиты государственной тайны?

4. Основные задачи информационной безопасности в соответствии с Концепцией национальной безопасности РФ.

5. Какие категории государственных информационных ресурсов определены в Законе "Об информации, информатизации и защите информации"?

6. Какая ответственность в Уголовном кодексе РФ предусмотрена за создание, использование и распространение вредоносных программ для ЭВМ?

7. Сколько классов защищенности СВТ от НСД к информации устанавливает РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?

8. Дайте характеристику уровням защиты СВТ от НСД к информации по РД "СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации"?

9. Классы защищенности АС от НСД по РД "АС. Защита от НСД к информации. Классификация АС и требования по защите информации".

10. Какие классы защищенных АС от НСД должны обеспечивать идентификацию, проверку подлинности и контроль доступа субъектов в систему?

11. Показатели защищенности межсетевых экранов.

12. Классы защищенности межсетевых экранов.

5.2.5. Типовые тестовые задания для оценки сформированности компетенции_ОПК-6

Тест 1

1. Информационная война - это...

А. злословие в адрес другого человека;

+Б. информационное противоборство с целью нанесения ущерба важным структурам противника, подрыв его политической и социальной систем, а также дестабилизации общества и государства противника;
В. акт применения информационного оружия.

2. Информационная безопасность - это...

+А. невозможность нанесения вреда свойствам объектам безопасности, обуславливаемым информацией и информационной инфраструктурой (защищенность от угроз);
Б. предотвращение зла наносимого государственным структурам;
В. проведение природоохранных мероприятий.

3. К понятию информационной безопасности НЕ относятся:

+А. природоохранные мероприятия;
Б. надежность работы компьютера;
В. сохранность ценных данных.

4. К объектам информационной безопасности на предприятии НЕ относятся:

А. информационные ресурсы;
Б. средства вычислительной и организационной техники;
+В. Конституция России.

5. Обеспечение безопасности информации - это...

А. одноразовое мероприятие;
+Б. комплексное использование всего арсенала имеющихся средств защиты;
В. разработка каждой службой плановых мер по защите информации.

6. Лингвистическое обеспечение информационной безопасности - это?

А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;
Б. нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации;
+В. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации.

7. Эргономическое обеспечение информационной безопасности - это?

А. антивирусные программы;
+Б. совокупность средств, обеспечивающих удобства работы пользователей аппаратных средств защиты информации;
В. комплекс математических методов, связанных с оценкой опасности технических средств.

8. Информационное обеспечение информационной безопасности — это?

А. совокупность специальных языковых средств общения специалистов и пользователей в сфере защиты информации;
Б. антивирусные программы;
+В. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы.

9. Организационное обеспечение информационной безопасности - это?

+А. реализация защиты информации структурными единицами, такими как: служба безопасности, служба режима и т.д.;
Б. совокупность средств;
В. нормативные документы по ИБ, требование которых являются обязательными в рамках сферы действия каждого подразделения.

10. К основным угрозам информационной безопасности НЕ относятся:

А. раскрытие конфиденциальной информации;
+Б. нарушение принципов экономической безопасности;
В. отказ от обслуживания.

11. Информационное оружие - это?

+А. комплекс технических средств, методов и технологий, направленных против управленческих систем;

Б. нормативно-правовая база по информационной безопасности;
В. комплекс индивидуального и общественного сознания.

12. Правовое обеспечение информационной безопасности - это..?

+А. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения;
Б. документированные сведения, лежащие в основе решения задач, обеспечивающих функционирование системы;
В. широкое использование технических средств защиты информации.

Тест 2

1. Экономическая информация является товаром?

+А. да;
Б. нет;
В. кроме конфиденциальных сведений.

2. К числу особенностей информации как товара НЕ относятся:

А. сохраняемость;
Б. несамостоятельность;
+В. самостоятельность.

3.Информация может составлять коммерческую тайну, если:

+А. к ней нет свободного доступа на законном основании;
Б. содержится в учредительных документах;
В. содержится в бухгалтерском балансах.

4.Не являются коммерческой тайной?

+А. сведения, содержащиеся в документах, дающие право заниматься предпринимательской деятельностью;
Б. сведения о научных разработках;
В. сведения о персонале предприятия.

б.Конфиденциальность компьютерной информацией - это?

А. предотвращение проникновения компьютерных вирусов в память ПЭВМ;
+Б. свойство информации быть известной только допущенным и прошедшим проверку (авторизацию) субъектам системы;
В. безопасное программное обеспечение.

6. Банковская тайна - это..?

+А. информация о банковском счете, вкладе, операциях по счету, о клиентах банка;
Б. информация о сотрудниках банка;
В. информация о режиме работы банка.

7.Объектами профессиональной тайны НЕ являются:

А. тайна страхования;
Б. врачебная тайна;
+В. бухгалтерский баланс.

Тест3

1. **Несанкционированным доступом является:**

А. недостаточное знание работниками предприятия правил защиты информации;
Б. слабый контроль за соблюдением правил защиты информации;
+В. хищение носителей информации и документальных отходов.

2. **Реализации угроз информационной безопасности способствуют:**

+А. болтливость;
Б. простудные заболевания;
В. Налоговый кодекс.

3. **Типовыми путями несанкционированного доступа к информации, являются:**

+А. дистанционное фотографирование;
Б. выход из строя ПЭВМ;
В. ураганы.

4. **Несанкционированным доступом к информации НЕ является:**
А. использование программных ловушек;
+Б. любительское фотографирование;
В. включение в библиотеки программ специальных блоков типа «троянский конь».
5. **К способам воздействия угроз на информационные объекты НЕ относятся:**
А. программно-математические;
Б. организационно-правовые;
+В. договорные отношения.
6. **Хакерная война - это?**
+А. атака компьютеров и сетей гражданского информационного пространства;
Б. использование информации для влияния на умы союзников и противников;
Б. блокирование информации, преследующее цель получить экономическое превосходство.
7. **Угрозы доступности данных возникают в том случае, когда?**
+А. объект не получает доступа к законно выделенным ему ресурсам;
Б. легальный пользователь передает или принимает платежные документы, а потом отрицает это, чтобы снять с себя ответственность;
8. случаются стихийные бедствия.
8. Внедрение компьютерных вирусов является следующим способом воздействия угроз на информационные объекты?
А. информационным;
Б. физическим;
+В. программно-математическим способом.
9; Логическая бомба - это?
+А. компьютерный вирус;
Б. способ ведения информационной войны;
В. прием, используемый в споре на философскую тему.
10. Объектом информационной атаки не является:
А. АИС в целом;
Б. каналы передачи данных;
+В. природоохранные мероприятия.
11. Под «маскарадом» понимается?
+А. выполнение каких-либо действий одним пользователем от имени другого пользователя;
Б. обработка денежных счетов при получении дробных сумм;
В. монополизация какого-либо ресурса системы.
12. «Люком» называется?
А. использование после окончания работы части данных, оставшиеся в памяти;
Б. передача сообщений в сети от имени другого пользователя;
+В. не описанная в документации на программный продукт возможность работы с ним.
13. «Мобильные» вирусы распространяются:
А. путем взлома программ ВЭВМ;
+Б. в виде «червей» и «троянцев» для мобильных телефонов;
В. по линии связи между узлами сети.
14.Для компьютерных преступлений НЕ характерна:
А. сложность сбора доказательств;
+Б. наличие достаточной следственной практики по раскрытию компьютерных преступлений в РФ;
В. высокая латентность.

Тест 4

1. Ассоциация вычислительной техники создана в
+А. 1947 году;
Б. 1964 году;
В. 2017 году.

1. Консорциум Всемирной Паутины оформлен

+А. в 1989 году;
Б. в 1994 году;
В. в 2017 году.

2. Международная организация по стандартизации это

+А. ISO;
Б. ACM;
В. ООН.

3. Проект международных стандартов приобретает статус международного стандарта, если за него проголосовало

А. 100% членов;
Б. 75% членов;
+В. 80% членов.

4. Альянс по безопасности сети Интернет создан в

+А. 2001 г.
Б. 2016 г.
В. 2017 г.

Тест 5

1. Доктрина Информационной безопасности принята в

А. 2012 году
Б. 2014 году
+В. 2016 году

2. В организационную основу системы обеспечения информационной безопасности РФ входит:

+А. Совет безопасности РФ;
Б. Министерство образования и науки РФ;
В. ЦРУ США.

3. К актам федерального законодательства по ИБ в РФ входят:

А. Приказы ФСБ;
Б. Международные стандарты;
+В. Конституция РФ.

4. Правовое обеспечение ИБ означает:

А. Защиту интересов физических и юридических лиц;
Б. Защиту интересов государства и общества;
+В. Все вышеперечисленное.

5. Масштабы компьютерной преступности в РФ

А. Неуклонно снижаются;
+Б. Возрастают;
В. Остаются из года в год неизменными.

6. Статья 23 Конституции РФ определяет:

А. Право на получение достоверной информации о состоянии окружающей среды;
+Б. Право на неприкосновенность частной жизни, личную и семейную тайну и иные сообщения;
В. Отказ в предоставлении гражданину информации.

7. В Налоговом кодексе РФ имеется:

А. ст. 139 «Служебная и коммерческая тайна»;
+Б. ст. 102 «Налоговые тайны»;
В. ст.946 «Тайна страхования».

8. Федеральный закон «Об информации, информационных технологиях и о защите информации»

А. пока не принят;
Б. принят в 2000 году;

+В. принят в 2006 году.

9. Федеральный закон «О персональных данных» принят:

+А. в 2006 году с изменениями на 1 января 2017 года;

Б. в 2009 году;

В. в 2016 году.

10. В какой статье УК предусматривается наказание за «Неправомерный доступ к компьютерной информации»?

+А. в ст.272;

Б. в ст.273;

В. в ст.274.

Типовые тестовые задания для оценки сформированности компетенции_ПК-3

Тест 1

1. Минимизация утечки информации через персонал это

А. организационно-технические средства защиты информации;

Б. организационно-экономические меры;

+В. организационно-административные меры.

1. К организации конфиденциального делопроизводства относится:

+А. организация документооборота;

Б. использование сертифицированных технических и программных средств;

В. проверка надежности сотрудников**.**

2. Организационное обеспечение информационной безопасности - это..?

+А. реализация защиты информации, осуществляемая службами безопасности режима, защита информации техническими средствами и др.;

Б. совокупность средств, обеспечивающих удобства работы пользователей;

В. нормативные документы по ИБ, требования которых являются обязательными в рамках сферы действия каждого подразделения.

3. С увольняющимися сотрудниками

+А. подписывается договор о не распространении конфиденциальности;

Б. обмениваются рукопожатием;

В. предлагают вернуться.

4. Организация документооборота предполагает:

А. исключение доступа к бумажной «стружке»;

Б. предупреждение не обоснованного ознакомления с документами;

+В. исключение не обоснованной рассылки.

5. Проведение организационно-экономических мероприятий предполагает:

+А. страхование информационных рисков;

Б. организацию пассивного противодействия техническими средствами;

В. обеспечения электронного документооборота.

Тест 2

1. Адрес электронной почты включает:

А. Логин.

Б. Символический адрес сервера и имя зоны.

+В. Все вышеперечисленное.

1. Электронная почта НЕ служит для:

А. Передачи текстовых сообщений в пределах Интернет.

+Б. Системы телеконференций.

А. Оповещения пользователей о наступлении определенных событий.

2. Информационными угрозами в Интернете НЕ является:

А. Несанкционированный доступ к сети организации.

Б. Сбор и мониторинг сетевой информации в интересах третьих лиц.

+В. Использование брандмауэра.

3. Для защиты электронной почты в Интернете используются:

А. Антивирусные программы.

+Б. Специальные протоколы (REM, CryptoAPi и др.)

В. Наиболее простое обозначение электронной почты (фамилия, паспортные данные и т.п.).

4. Основные сервисы системы Интернет:

А. WorldWideWeb (WWW).

Б. Программы-браузеры и системы телеконференций.

+В. Все вышеперечисленное.

5. К серверам системы Интернет НЕ относятся:

+А. Программа печати учетных документов.

Б. Программа пересылки файлов.

В. Система информационного поиска сети Интернет.

6. Адрес электронной почты имеет вид:

+А. логин@символический адрес сервера.имя зоны;

Б. логин.имя зоны;

В.логин.

7. Межсетевой экран - это

+А. Брандмауэр (Firewalls);

Б. Фильтр;

8. Антивирусная программа.

8. Чтобы избавиться от мобильного вируса:

+А. Нужно пользоваться клавишным мобильником.

Б. Приобрести самый дорогостоящий мобильник.

В. Познакомиться с хакером.

9. Недостатком информирования с симметричным ключом:

А. Легко реализовать аппаратно;

Б. Быстрота;

А. Оба ключа одинаковы.

10. Преимущества шифрования с открытым (ассиметричным) ключом

А. Работает медленно;

Б. Требует больших вычислительных мощностей;

+В. используется два разных ключа.

Тест 3

1. Каждую систему защиты следует разрабатывать индивидуально, учитывая:

А. Организационную структуру организации;

Б. Объем и характер информационных потоков;

+В. Все вышеперечисленное.

1. Первый этап построения системы защиты:

А. Планирование;

+Б. Анализ;

А. Реализация системы защиты.

2. По способу осуществления всех мер обеспечения безопасности подразделяются на:

А. Правовые и морально-этические;

Б. Административные, физические, аппаратные и программные;

+В. Все вышеперечисленное.

3. Чаще всего применяется способ реализации защиты:

А. «Встроенная»;

+Б. Комбинированная;

А. «Добавленная».

4. Этапы сопровождения это:
+А. Контроль работы системы, регистрация происходящих в ней событий и их анализ;
Б. Планирование системы защиты;
А. Реализация системы защиты.
6. Политика безопасности входит в
А. Анализ рисков;
+Б. План защиты;
А. Управление доступом.
6. План обеспечения непрерывной работы и восстановления включает:
А. Что и когда должно быть сделано;
Б. Кем и как это должно быть сделано;
+В. Все вышеперечисленное.
8. Относится к вложениям в информационную безопасность следует как:
1. К затратам;
+Б. к инвестициям;
8. К неизбежным потерям.
8. ROI это:
+А. процентное отношение прибыли от проекта к инвестициям;
Б. разделение затрат на прямые и косвенные;
8. средневзвешенная стоимость капитала.
Критерии оценок
«превосходно» - 96-100% правильных ответов;
«отлично» — 86-95% правильных ответов;
«очень хорошо» - 81-85% правильных ответов;
«хорошо» - 66-80% правильных ответов;
«удовлетворительно» - 56-65% правильных ответов.
«неудовлетворительно» - 46-55% правильных ответов;
«плохо» - 45% и меньше правильных ответов.

6. Учебно-методическое и информационное обеспечение дисциплины

а) основная литература:
1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326
2. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : Учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - М.: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2
3. Информационная безопасность: Учебное пособие/Партыка Т. Л., Попов -е изд., перераб. и доп. - М.: Форум, НИЦ ИНФРА-М, 2016. - 432 с.: 60x90 1/16. - (Профессиональное образование) (nepenneT)ISBN 978-5-91134-627-0, 200 экз. http://znaniurn.com/bookread2.php?book=516806
4. Сычев, Ю. Н. Стандарты информационной безопасности. Защита и обработка конфиденциальных документов : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2021. — 223 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_5cc15bb22f5345.11209330. - ISBN 978-5-16-014397-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189349

б) дополнительная литература:
1. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - 2-е изд.,

доп. - М.: Форум: НИЦ ИНФРА-М, 2015. - 240 с.: ил.; 60х90 1/16. - (Высшее образование: Бакалавриат). (обложкаДБВИ 978-5-00091-007-8, 300 экз. http://znanium.com/bookread2.php?book=491597

2. Информационная безопасность и защита информации: Учебное посо- бие/Баранова Е. К., Бабаш А. В., 3-е изд. - М.: ИЦ РИОР, НИЦ ИНФРА-М, 2016. -Рабочая программа и ФОС составлены в соответствии с требованиями ОС ННГУ по направлению подготовки 38.03.01 «Экономика», профиль «Экономика, международный бизнес и предпринимательство».

в) программное обеспечение и Интернет-ресурсы (в соответствии с содержанием дисциплины)

A. www.gks.ru / Федеральная служба государственной статистики.
B. Операционная система Microsoft Windows
C. Прикладное программное обеспечение Microsoft Office
D. Справочно-правовая система «КонсультантПлюс»

7. Материально-техническое обеспечение дисциплины

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой, оснащенные оборудованием и техническими средствами обучения: компьютером, проектором или ЖК-телевизором, акустической системой и микрофоном (при необходимости), а также доской.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечены доступом в электронную информационно-образовательную среду.

Программа составлена в соответствии с требованиями ОС ННГУ по направлению 38.03.01 «Экономика», направленность (профиль) программы «Цифровые системы учета, анализа и аудита».

Авторы:

к.э.н., профессор кафедры «Информационных технологий

и инструментальных методов в экономике» В.Н.Ясенев

к.э.н., доцент кафедры «Информационных технологий

и инструментальных методов в экономике» А.В.Дорожкн

Рецензенты:

д.э.н., профессор, зам.

генерального директора федерального казенного учреждения Н. Ф. Поляков

Программа утверждена решением президиума ученого совета ННГУ от «14» декабря 2021 г., протокол № 4