ПРИЛОЖЕНИЕ 1
к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Экономическая безопасность, анализ и учет»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б1.В.ДВ.04.01 «ЗАЩИТА ИНФОРМАЦИИ В ХОЗЯЙСТВУЮЩИХ СУБЪЕКТАХ»

Специальность
38.05.01 Экономическая безопасность

Специализация
Экономическая безопасность хозяйствующих субъектов

Уровень подготовки
специалитет

Квалификация выпускника – экономист

Формы обучения – очная

Рязань 2023 г

1 ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части основной образовательной программы.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций, обучающихся целям и требованиям основной образовательной программы в ходе проведения текущего контроля и промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных и профессиональных компетенций, приобретаемых обучающимися в соответствии с этими требованиями.

Контроль знаний проводится в форме текущего контроля и промежуточной аттестации.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи. К контролю текущей успеваемости относятся проверка знаний, умений и навыков, приобретённых обучающимися на практических занятиях.

На практических занятиях допускается использование либо системы «зачтено – не зачтено», либо рейтинговой системы оценки, при которой, например, правильно решенная задача оценивается определенным количеством баллов. При поэтапном выполнении учебного плана баллы суммируются. Положительным итогом выполнения программы является определенное количество набранных баллов.

Текущий контроль успеваемости проводится с целью определения степени усвоения учебного материала, своевременного выявления и устранения недостатков в подготовке обучающихся и принятия необходимых мер по совершенствованию методики преподавания учебной дисциплины (модуля), организации работы обучающихся в ходе учебных занятий и оказания им индивидуальной помощи.

Промежуточная аттестация студентов проводится на основании результатов выполнения ими ИДЗ, практических и лабораторных работ.

По итогам изучения разделов дисциплины «Защита информации в хозяйствующих субъектах», обучающиеся в конце учебного семестра проходят промежуточную аттестацию. Форма проведения аттестации – экзамен в устной или письменной формах. Перечни вопросов, задач, примеров, выносимых на промежуточную аттестацию, составляются с учётом содержания тем учебной дисциплины.

В процессе подготовки к зачету экзаменуемый может составить в письменном виде план ответа, включающий в себя определения, выводы формулы, рисунки и т.п.

Паспорт фонда оценочных средств по дисциплине

Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или её части)	Вид, метод, форма оценочного мероприятия
1. Защита информации.	ОПК-6	Экзамен
2. Цели и направления защиты информации.	ОПК-6	Экзамен
3. Объекты защиты информации.	ОПК-6	Экзамен
4. Государственная система информационной безопасности.	ОПК-6	Экзамен
5. Защита информации в автоматизированных системах.	ОПК-6	Экзамен
6. Контроль	ОПК-6	Экзамен

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1) пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;

2) продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;

эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

Перечень компетенций с указанием этапов их формирования

При освоении дисциплины «Защита информации в хозяйствующих субъектах» формируются компетенции: ОПК-6 (индикаторы ОПК-6.2.

Указанные компетенции формируются в соответствии со следующими этапами:

- формирование и развитие теоретических знаний, умений, навыков, предусмотренных данной компетенцией (лекционные занятия, самостоятельная работа студентов);
- приобретение и развитие практических знаний, умений, навыков, предусмотренных компетенцией (практические занятия, лабораторные работы, самостоятельная работа студентов);

закрепление теоретических знаний, умений, навыков, предусмотренных

компетенцией, в ходе решения конкретных задач на практических занятиях, выполнения лабораторных работ, а также в процессе прохождения промежуточной аттестации.

Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Сформированность компетенции в рамках освоения данной дисциплины оценивается по двоичной шкале:

0 – компетенция не сформирована (выявляется менее 50% приведённых знаний, умений и навыков);

1 – компетенция сформирована (выявляется 50% и более приведённых знаний, умений и навыков).

Уровень сформированности компетенции на различных этапах её формирования в процессе освоения дисциплины «Защита информации в хозяйствующих субъектах» оценивается в ходе текущего контроля успеваемости и промежуточной аттестации и представлен различными видами оценочных средств.

Оценке сформированности в рамках данной дисциплины подлежат компетенции и индикаторы:

ОПК-6: - Способен использовать современные информационные технологии и программные средства при решении профессиональных задач;

– ОПК-6.2 - Применяет в профессиональной деятельности принципы работы современных информационных технологий в сетях различного уровня, принципы организации различных сервисов сети Интернет.

Преподавателем оценивается содержательная сторона и качество изложения и аргументирования материалов на этапах промежуточной аттестации, итоги написания контрольной работы, ответы студента на вопросы по соответствующим видам занятий при текущем контроле на практических занятиях:

- контрольные опросы;
- контрольная работа;
- задания по практическим занятиям.

Принимается во внимание **знания** обучающимися:

- потенциальных угроз безопасности информации;
- методов, средств и стандартов защиты информации.

наличие **умений**:

- определять угрозы безопасности информации автоматизированных систем;
- определять средства и способы защиты информации в автоматизированных системах.

–

обладание:

- навыками разработки требований к системе защиты информации автоматизированных систем;
- навыками применения соответствующих мер защиты информации в автоматизированных системах.

Критерии оценивания компетенций (результатов)

1. Уровень усвоения материала, предусмотренного программой.
2. Умение анализировать материал, устанавливать причинно-следственные связи.
3. Качество ответа на вопросы: полнота, аргументированность, убежденность, логичность.
4. Содержательная сторона и качество материалов, приведенных в отчетах студента по практическим занятиям.
5. Использование дополнительной литературы при подготовке ответов.

Формой промежуточной аттестации по дисциплине «Защита информации в хозяйствующих субъектах» является экзамен с оценкой (в устной или письменной формах), оцениваемый по принятой в ФГБОУ ВО РГРТУ четырехбальной системе: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Критерии оценивания промежуточной аттестации представлены в таблице 1.

Таблица 1. Критерии оценивания промежуточной аттестации

Шкала оценивания	Критерии оценивания
«отлично»	**студент должен:** продемонстрировать глубокое и прочное усвоение знаний материала; исчерпывающе, последовательно, грамотно и логически стройно изложить теоретический материал; правильно формулировать определения; уметь сделать выводы по излагаемому материалу; безупречно ответить не только на вопросы билета, но и на дополнительные вопросы в рамках рабочей программы дисциплины; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой.
«хорошо»	**студент должен:** продемонстрировать достаточно полное знание материала; продемонстрировать знание основных теоретических понятий; достаточно последовательно, грамотно и логически стройно излагать материал; уметь сделать достаточно обоснованные выводы по излагаемому материалу; ответить на все вопросы билета; продемонстрировать умение правильно выполнять практические задания, предусмотренные программой, при этом возможно допустить непринципиальные ошибки.
«удовлетворительно»	**студент должен:** продемонстрировать общее знание изучаемого материала; знать основную рекомендуемую программой дисциплины учебную литературу; уметь строить ответ в соответствии со структурой излагаемого вопроса; показать общее владение понятийным аппаратом дисциплины; уметь устранить допущенные погрешности в ответе на теоретические вопросы и/или при выполнении практических заданий под руководством преподавателя, либо (при неправильном выполнении практического задания) по указанию преподавателя выполнить другие практические задания того же раздела дисциплины.
«неудовлетворительно»	**ставится в случае:** незнания значительной части программного материала; невладения понятийным аппаратом дисциплины; существенных ошибок при изложении учебного материала; неумения строить ответ в соответствии со структурой излагаемого вопроса; неумения делать выводы по излагаемому материалу. Оценка «неудовлетворительно» ставится студентам, которые не могут продолжить обучение по образовательной программе без дополнительных занятий по соответ-

	ствующей дисциплине (формирования и развития компетенций, закрепленных за данной дисциплиной). Оценка «неудовлетворительно» выставляется также, если студент после начала экзамена отказался его сдавать или нарушил правила сдачи экзамена (списывал, обманом пытался получить более высокую оценку и т.д.).

4. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Для укрепления предусмотренных компетенциями, закреплёнными за дисциплиной знаниями, умениями и навыками, предусматривается текущая проверка путём опроса, выполнения заданий на практических занятиях, проверка знаний, умений и навыков, приобретаемых студентами самостоятельно, выполнения контрольной работы, проверка на промежуточной аттестации.

Фонд оценочных средств промежуточной аттестации, проводимой в форме экзамена, включает: типовые теоретические вопросы; типовые практические вопросы; дополнительные вопросы.

Оценочные средства приведены ниже. Разрешается и иная формулировка вопроса или примера, без изменения его смысла или содержания, например, дробление, изменение условий или иное.

Типовые тестовые вопросы:

1. Что относится к физическим средствам защиты информации?

+ средства, которые реализуются в виде автономных устройств и систем;

устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;

программы, предназначенные для выполнения функций, связанных с защитой информации.

2. Что относится к техническим средствам защиты информации?

устройства, встраиваемые непосредственно в аппаратуру АС или устройства, которые сопрягаются с аппаратурой АС по стандартному интерфейсу;

это программы, предназначенные для выполнения функций, связанных с защитой информации;

+ средства, которые реализуются в виде электрических, электромеханических и электронных устройств.

3. Что такое несанкционированный доступ?

+ доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

правила и положения, выработанные в организации для обхода парольной защиты;

вход в систему без согласования с руководителем организации.

4. Что такое целостность информации?

свойство информации, заключающееся в возможности ее изменения любым субъектом;

свойство информации, заключающееся в возможности изменения только

единственным пользователем;

+ свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

5. Под информационной безопасностью понимают;

защиту от несанкционированного доступа;

+ защиту информации от случайных и преднамеренных воздействий естественного и искуственного характера;

защиту информации от компьютерных вирусов.

6. Что такое аутентификация?

проверка количества переданной и принятой информации;

нахождение файлов, которые изменены в информационной системе несанкционированно;

+ проверка подлинности идентификации пользователя, процесса, устройства или другого компонента системы (обычно осуществляется перед разрешением доступа).

7. Верификация это:

проверка принадлежности субъекту доступа предъявленного им идентификатора;

+ проверка целостности и подлинности информации, программы, документа;

присвоение имени субъекту или объекту.

8. Утечка информации это:

несанкционированное изменение информации, корректное по форме, содержанию, но отличное по смыслу;

+ ознакомление постороннего лица с содержанием секретной информации;

потеря, хищение, разрушение или неполучение переданных данных.

9. Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации называется:

шифруемой;

достоверной;

+ защищаемой.

10. Абстрактное содержание какого-либо высказывания, описание, указание, сообщение либо известие – это:

текст;

данные;

+ информация.

11. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется:

+ угрозой;

опасностью;

предостережением.

12. Из каких компонентов состоит программное обеспечение любой универсальной компьютерной системы?

операционной системы, сетевого программного обеспечения;

+ операционной системы, сетевого программного обеспечения и системы управления базами данных;

сетевого программного обеспечения и системы управления базами данных.

13. Комплекс мер и средств, а также деятельность на их основе, направленная на выявление, отражение и ликвидацию различных видов угроз безопасности объектам защиты называется:

системой угроз;

+ системой защиты;

системой уничтожения.

14. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется:

защитой информации;

+ политикой безопасности;

организацией безопасности.

15. Какая угроза возникает в результате технологической неисправности за пределами информационной системы?

информационная;

+ техническая;

сетевая.

16. Что такое компьютерный вирус?

+ разновидность программ, которые способны к размножению;

разновидность программ, которые самоуничтожаются;

разновидность программ, которые не работают.

17. Как подразделяются вирусы в зависимости от деструктивных возможностей?

сетевые, файловые, загрузочные, комбинированные;

+ безвредные, неопасные, опасные, очень опасные;

резидентные, нерезидентные.

18. К угрозам какого характера относятся действия, направленные на сотрудников компании или осуществляемые сотрудниками компании с целью получения конфиденциальной информации или нарушения функции бизнес-процессов?

физического;
+ организационного;
системного.

19. Метод пароля и его модификация, метод вопрос-ответ - это методы:

идентификации;
+ аутентификации;
защиты данных.

20. Нежелательная цепочка носителей информации, один или несколько из которых являются правонарушителем или его специальной аппаратурой называется:

каналом несанкционированного доступа;
+ каналом утечки информации;
каналом искажения информации.

Примеры типовых вопросов:

1. Информация – сведения (сообщения, данные) независимо от формы их ……. (представления).
2. Безопасность информации – состояние защищенности информации, при котором обеспечивается ее конфиденциальность, целостность, доступность, а также ……. (другие заданные характеристики ее безопасности).
3. Конфиденциальность информации – защищенность информации от несанкционированного, не имеющего законного основания ……. (получения).
4. Целостность информации – защищенность информации от несанкционированного, не имеющего законного основания …… (изменения).
5. Доступность информации – возможность своевременного санкционированного, имеющего законное основание …….. (получения доступа к информации).

Оценочные материалы составлены в соответствии с рабочей программы дисциплины «Защита информации в хозяйствующих субъектах» по специальности 38.05.01 «Экономическая безопасность».

Составил
Ст. преподаватель кафедры
«Информационная безопасность» Н.А. Колесенков