Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине Б1.В.ДВ.6.1 Защита информации в офисе

Общие сведения

1.	Кафедра	физики, информатики и информационных технологий
2.	Направление подготовки	43.03.02 Туризм (Технология и организация туроператоских и турагентских услуг), ОФО
3.	Дисциплина (модуль)	Б1.В.ДВ.6.1 Защита информации в офисе
4.	Тип заданий	Тесты, лабораторные работы, эссе, доклады, опросы
5.	Количество этапов формирования компетенций (ДЕ, разделов, тем и т.д.)	5

Перечень компетенций

ОПК-1: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности, использовать различные источники информации по объекту туристского продукта.

Критерии и показатели оценивания компетенций

Знания: – понятие компьютерных преступлений, их разновидности; – виды информации, защищаемой законодательством; – основные нормативно-правовые и законодательные акты, регулирующие мероприятия по защите информации на территории Российской Федерации; – основные направления обеспечения безопасности информационных ресурсов; – понятие Государственной тайны; – понятие электронной цифровой подписи; – виды угроз безопасности информации и информационных атак, меры их предупреждения и реагирования в случае возникновения; – основные каналы утраты информации; – наиболее уязвимые участки офисной деятельности с точки зрения обеспечения ИБ; – программные и аппаратные возможности обеспечения информационной безопасности в офисе; – основные направления и этапы аналитической работы в сфере безопасности информации в офисе.
Умения: – находить и анализировать необходимый законодательный акт в соответствии с возникшей профессиональной задачей; – определять конфиденциальную информацию. – осуществлять анализ степени защищенности информации;

– использовать основные технологии защиты данных; – осуществлять подбор средств обеспечения ИБ с учетом специфики канала утраты информации; – осуществлять защиту документов от внутренних ИТ-угроз без использования специальных средств; – создавать и настраивать учетные записи пользователей с целью обеспечения ИБ; – использовать криптографические методы защиты информации; – выделять актуальные направления информационно-аналитической работы.
Навыки: – владения приемами анализа нормативно-правовой документации с целью получения необходимой информации; – владения приемами реализации технологий защиты данных; – владения технологиями выявления существующих угроз безопасности информации и возможных информационных атак; – владения методами защиты документов от внутренних ИТ-угроз; – владения теоретическими основами составления аналитических отчетов.

Этапы формирования компетенций

1. Нормативно-правовое обеспечение информационной безопасности.
2. Основные направления обеспечения безопасности информационных ресурсов.
3. Угрозы безопасности информации и информационные атаки.
4. Обеспечение безопасности информации на наиболее уязвимых участках офисной деятельности.
5. Информационно-аналитическая работа в сфере информационной безопасности и системе защиты информационных ресурсов.

Шкала оценивания в рамках балльно-рейтинговой системы
«2» - 60 баллов и менее «3» - 61-80 баллов «4» - 81-90 баллов «5» - 91-100 баллов

Критерии и шкалы оценивания

1) Активность на лабораторных занятиях

Максимальное количество баллов за активность на лабораторных занятиях – 7 баллов. Данный вид деятельности включает в себя продуктивность работы студента во время лабораторного занятия. Оценивание осуществляется с использованием автоматизированного элемента в системе управления обучением пропорционально деятельности (Выполнено 100% работы; Выполнено 50% работы; Не работал).

2) Лабораторные работы

Лабораторные работы по дисциплине реализованы в форме лабораторных разработок с перечнем заданий, требующих выполнения и предоставления на проверку конечного результата работы (в виде одного или нескольких файлов, текстового сообщения).

Максимальное количество баллов за лабораторную работу – 5 баллов.

Оценивание лабораторных работ осуществляется следующим образом:

– 5 баллов – все задания выполнены правильно, результат представлен в требуемом виде (либо имеются 1-2 замечания по оформлению);
– 3-4 балла – в выполненных заданиях имеются 1-2 ошибки, имеются неточности в представлении результатов, имеются 2-3 замечания по оформлению;

- 1-2 балла – в выполненных заданиях имеется 3 и более ошибок, результат работы оформлен небрежно, не соответствует требованиям лабораторной работы;
- 0 баллов – результат работы не соответствует заданию или не представлен на проверку.

3) Подготовка доклада

Максимальное количество баллов за доклад – 10 баллов. Оценивание доклада включает в себя следующие показатели:

- распечатанный текст доклада, оформленный в соответствии с требованиями к оформлению и объему – max 5 баллов (0 баллов – нет доклада вообще, 1-2 балла – доклад представлен, но есть много недочетов и несоответствий, 3-4 балла – доклад представлен, но есть незначительные недочеты, 3 балла – замечаний нет);
- подготовка презентации, сопровождающей выступление, – max 3 балла (0 баллов – презентация не подготовлена, 1-2 балла – презентация подготовлена, но имеются недочеты, 3 балла – замечаний нет) – оценивается только на защите;
- выступление с защитой доклада, ответы на вопросы – max 2 балла (0 баллов – не участвовал в защите, 1 балл – выступление удовлетворительное с недочетами, 2 балла – выступление удовлетворение, на все вопросы даны ответы).

4) Подготовка эссе

Максимальное количество баллов за эссе – 3 балла. Оценивание эссе включает в себя следующие показатели:

- *содержание эссе* – 1,5 балла (тема раскрыта полностью; присутствуют рассуждения и умозаключения студента; объем работы соответствует требованиям); 0,5-1,4 балла (тема раскрыта слабо, не затронуты (или слабо затронуты) основные аспекты темы; мнение студента по данному вопросу представлено кратко; объем работы соответствует требованиям); 0,1-0,4 балла (тема раскрыта поверхностно; точка зрения студента не представлена; объем работы меньше указанного в требованиях); 0 баллов – работа не представлена на проверку;
- *оформление эссе* – 1-1,5 балла (все требования к оформлению доклада соблюдены или допущены 1-2 неточности); 0,1-0,9 балла (допущено 3 и более неточностей в оформлении либо текст не оформлен в соответствии с требованиями).

5) Зачетное задание

Максимальное количество баллов на зачете – 40 баллов. Оценивание на зачете включает в себя следующие показатели:

- *теоретическая часть* – максимально 32 балла – оценивание осуществляется автоматически системой тестирования в Moodle в зависимости от количества правильных и частично правильных ответов; тест считается зачтенным, если студенты ответили правильно на 61% (и более) всех вопросов;
- *практическая часть* – максимально 8 баллов – максимально 8 баллов – начисляется по 1 баллу за каждую зачтенную (т.е. оцененную на 50% и более от максимально возможной оценки) лабораторную работу; выставление баллов за практическую часть осуществляется один раз на зачетном занятии по факту выполненных лабораторных работ.

Типовые контрольные задания и методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

1) Типовое тестовое задание для зачета:

Тема 1. Нормативно-правовое обеспечение информационной безопасности.

1. К видам информации, защищаемой законодательством РФ, относятся (выберите несколько вариантов):
    a. персональные данные;
    b. служебная тайна;
    c. список кандидатов на выборы в Госдуму;
    d. справочная информация организации.

Тема 2. Основные направления обеспечения безопасности информационных ресурсов.

2. Установите соответствие между понятиями и их определениями:

А1. Информационные продукты – это…	А2. …стоимостная категория информации, характеризующая конкретный размер прибыли при ее использовании или размер убытков при ее утрате.
Б1. Ценность информации – это…	Б2. … действия субъектов (собственников и владельцев ресурсов) по обеспечению пользователей информационными продуктами.
В1. Информационная услуга – это…	В2. … документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

Тема 3. Угрозы безопасности информации и информационные атаки.

3. Закончите определение: лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (агентов иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, отдельных преступных элементов, лиц, сотрудничающих со злоумышленниками, психически больных и пр.), называется …

Тема 4. Обеспечение безопасности информации на наиболее уязвимых участках офисной деятельности.

4. Если пользователи создают свои собственные пароли, каких рекомендаций они должны придерживаться (выберите все возможные варианты)?
    a. использовать максимально возможное количество символов в пароле;
    b. использовать в качестве пароля имя супруга/супруги, ребенка или кличку собаки (чтобы не забыть пароль);
    c. использовать хотя бы одну прописную букву, один символ нижнего регистра, одну цифру и один допустимый не алфавитно-цифровой символ;
    d. использовать пароль, который трудно угадать по смыслу.

Тема 5. Информационно-аналитическая работа в сфере информационной безопасности и системе защиты информационных ресурсов.

5. Напишите развернутый ответ на вопрос: что, на ваш взгляд, является информационно-аналитической работой?

Ключ к тестовым заданиям:

№ вопроса	Правильный вариант ответа
1.	a, b
2.	А1-В2 Б1-А2 В1-Б2
3.	злоумышленником
4.	c, d
5.	Это работа по изучению наиболее уязвимых объектов конфиденциальной информации, каналов ее санкционированного распространения и возможных угроз в отношении нее с целью предотвращения нарушения ее конфиденциальности.

2) Типовое задание лабораторной работы:

Подготовьте файл с таблицей для анализа законодательных актов из приведенного ниже списка. В таблице отразите такие параметры, как название законодательного акта, понятия, объекты, цели, основные положения. Выберите не менее пяти, наиболее важных на ваш взгляд, законодательных актов и заполните таблицу.

3) Требования к докладу:

Требования к оформлению доклада:

1. Объем доклада – 5 страниц (без титульного листа и списка источников).
2. Титульный лист должен быть оформлен по образцу (имеется файл с образцом).
3. Основной текст работы оформлен в соответствии с требованиями, указанными ниже.
4. В случае использования в тексте таблиц и/или рисунков на каждый объект должна быть ссылка в тексте работы. Например, «... основные виды программных средств представлены ниже (см. Таблица 1)» или «... схему передачи информации можно увидеть на рис. 1».
5. Количество источников должно быть не менее трех, на все должны быть ссылки внутри текста.
6. Список используемых источников должен быть оформлен в соответствии с требованиями, указанными ниже.

Для оформления основного текста работы:

1. Шрифт – TimesNewRoman, размер – 14 пт.
2. Абзац: междустрочный интервал – 1,5; выравнивание – «по ширине»; абзацный отступ – 1,25 см.
3. Оформление рисунков (при необходимости): выравнивание рисунка – «по центру», подпись рисунка – «Рис. №. Название рисунка»; шрифт для подписи рисунка – TimesNewRoman, размер – 12 пт.
4. Оформление таблиц (при необходимости): выравнивание таблицы – «по центру»; шрифт внутри таблицы – TimesNewRoman, размер – 11-12 пт.; выравнивание текста внутри таблицы – на усмотрение пользователя; подпись таблицы располагается над таблицей и состоит из двух частей: «Таблица №» – выравнивание по правому краю и «Название таблицы» – выравнивание по правому краю или по центру.

Для оформления источников (в соответствии с ГОСТ 2008):

1. Источники должны быть расположены в алфавитном порядке и пронумерованы.
2. В тексте доклада ссылка на источник выполняется в виде: [№], где № – номер источника в общем списке.
3. Если в тексте используется дословная цитата, то она должна быть взята в кавычки, а в ссылке на источник указана страница: [5, с.15].

4) Примерные темы докладов:

- Структура системы защиты на основе программно-аппаратных средств вычислительной системы.
- Общая организация защиты от компьютерных вирусов. Использование средств аппаратного и программного контроля.
- Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств.
- Средства операционной системы по диагностированию и локализации несанкционированного доступа к ресурсам вычислительной сети.
- Угрозы информационно-программному обеспечению, характерные только для распределенной вычислительной среды.
- Использование межсетевых экранов (брандмауэров) для защиты информации в локальных вычислительных сетях.

5) Требования к эссе на тему «Защита информации в моей профессиональной деятельности»:

1. Объем текста – 150-200 слов.
2. Работа должна содержать примеры и личную точку зрения автора. Возможна проверка работы в системе Антиплагиат.
3. Оформление текста:
   - шрифт Arial или TimesNewRoman, 14 пт;
   - междустрочный интервал – 1,5;
   - выравнивание основного текста – «по ширине»;
   - переносы разрешены;
   - заголовок – все прописные, полужирный, выравнивание «по центру»;
   - автор – расположение под заголовком, полужирный курсив, выравнивание «по центру».

6) Вопросы к зачету:

Зачет осуществляется в форме тестирования. Вопросы, входящие в контрольную тестовую базу, охватывают материал, представленный в содержании дисциплины (см. п.6):

1. Понятие и виды информации, защищаемой законодательством РФ.
2. Понятие компьютерных преступлений и их классификация.
3. Уголовно-правовая характеристика компьютерных преступлений.
4. Компьютерные вирусы: понятие и классификация.
5. Способы борьбы с компьютерными вирусами. Профилактические мероприятия.
6. Информационные ресурсы, продукты и услуги.
7. Информационная безопасность и политика безопасности – понятие и особенности.
8. Технологии защиты данных.
9. Государственная тайна и система ее защита.
10. Конфиденциальная информация и ее защита.
11. Электронная цифровая подпись.
12. Угрозы конфиденциальной информации.
13. Каналы утраты информации.
14. Информационные атаки.
15. Защита информации при проведении совещаний и переговоров.

16. Защита информации при работе с посетителями.
17. Защита информации в работе кадровой службы.
18. Защита документов от внутренних ИТ-угроз – общие подходы.
19. Управление учетными записями пользователей.
20. Администрирование общих папок как средство организации информационной безопасности.
21. Ограничение доступа к содержимому электронных документов.
22. Настройка параметров безопасности и параметров подключения к Интернету.
23. Информационно-аналитическая работа, направления и этапы.
24. Методы аналитической работы.
25. Система защиты конфиденциальной информации.