

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Локтионова Оксана Геннадьевна
Должность: проректор по учебной работе
Дата подписания: 08.02.2021 16:53:45
Уникальный программный ключ:
0b817ca911e6668abb13a50926d70a5b11eabb573e9431f4448516b564089

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Юго-Западный государственный университет»
(ЮЗГУ)

Кафедра информационной безопасности



УТВЕРЖДАЮ
Проректор по учебной работе
О.Г. Локтионова
_____ 2017 г.

**Составление обзорного документа по сертифицированным
продуктам в заданной области информационной безопасности**

Методические указания по выполнению практической работы

Курск 2017

Цель работы

Целью данной лабораторной работы является обзорного документа по сертифицированным продуктам в заданной области информационной безопасности.

Требования к выполнению задания:

В ходе выполнения задания необходимо провести анализ сертифицированных продуктов в заданной области информационной безопасности. После этого следует определить, какие средства защиты являются наиболее приемлемыми для использования в системах защиты. По результатам анализа оформить отчет.

При поиске средств защиты в заданной области, искать сертификацию на соответствие требованиям:

№	Вид СЗИ	Предназначение средства (область применения)
1.	Средства защиты от несанкционированного доступа	соответствует документу «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа»
2.	Межсетевые экраны	соответствует документу «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатель защищенности от несанкционированного доступа к информации»
3.	Антивирусные средства	соответствует документу «Требования к средствам антивирусной защиты»
		соответствует документу «Профиль защиты средств антивирусной защиты»
4.	Средства криптографической защиты	«может использоваться для криптографической защиты»
5.	Средства обнаружения вторжений	соответствует документу «Требования к системам обнаружения вторжений»
		соответствует документу «Профиль защиты систем обнаружения вторжений уровня узла»
6.	Средства контроля защищенности (автоматизированного анализа защищенности и обнаружения уязвимостей автоматизированных систем)	«является средством анализа защищенности и обнаружения уязвимостей»
7.	Средства резервного	«предназначен для создания

№	Вид СЗИ	Предназначение средства (область применения)
	копирования	автоматизации процессов резервного копирования»

1. Задание:

Примерный перечень заданий:

1. Определить, кто из регуляторов проводит сертификацию в заданной области средств защиты информации
2. Пользуясь сайтами регуляторов в области защиты информации Федеральной службы безопасности (<http://clsz.fsb.ru/>) и Федеральной службы по техническому и экспортному контролю (<http://fstec.ru/>) выбрать средства защиты по направлению (номер в списке группы по порядку):
 - 2.1. Средства защиты от несанкционированного доступа;
 - 2.2. Межсетевые экраны;
 - 2.3. Антивирусные средства;
 - 2.4. Средства криптографической защиты;
 - 2.5. Средства обнаружения вторжений;
 - 2.6. Средства контроля защищенности;
 - 2.7. Средства резервного копирования;
 - 2.8. Свой вариант (по согласованию).
3. Сделать сравнительный анализ всех средств защиты в форме таблицы.

№	Название	Срок действия	Выполняемые функции	Изготовитель

4. Из полученного списка и определить наиболее привлекательные средства защиты. Объяснить почему.
5. Найти сертификаты для выбранных средств защиты информации (на сайтах производителей).
6. Сопоставить данные из сертификата выбранного средства защиты и требования руководящего документа Гостехкомиссии или другого соответствующего документа (найти ссылку в сертификате).

2. Требования к отчету:

Отчет должен содержать:

1. титульный лист;
2. цель работы;
3. заданную область информационной безопасности;
4. сравнительный анализ средств защиты;
5. выбранное оптимальное средство защиты, обоснование почему и сертификат на него (скачать на сайте производителя СЗИ);
6. Перечень документов, на соответствие которым сертифицирован продукт;
7. выводы по проделанной работе.

3. Вопросы:

1. Как проводится сертификация средств защиты информации?
2. Что показывают характеристики данного средства защиты?
3. Какой регулятор контролирует данную область информационной безопасности?
4. Какая основная информация содержится в сертификате?

Список дополнительной литературы:

1. Справочно-поисковая система «Консультант Плюс»;
2. Справочно-поисковая система «Гарант»;
3. <http://clsz.fsb.ru/>
4. <http://fstec.ru/>