Министерство образования Российской Федерации

Пензенский государственный университет

Кафедра «САПР»

**ОТЧЁТ**

По лабораторной работе №5

По курсу «Информационная безопасность САПР»

На тему «Стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации»

Выполнил:

ст. гр.20ВВ2.1

Горбунов Никита

Проверила:

Эпп В. В.

Пенза, 2022

Список актуальных угроз:

|  |  |
| --- | --- |
| Наименование угрозы | Актуальность угрозы |
| 2.1.1 Кража ПЭВМ | Актуальная |
| 2.1.2 Кража носителей информации | Актуальная |
| 2.1.3 Кража ключей доступа | Актуальная |
| 2.1.4 Кражи, модификации, уничтожения информации | Актуальная |
| 2.1.5 Вывод из строя узлов ПЭВМ, каналов связи | Актуальная |
| 2.2.1 Действия вредоносных программ (вирусов) | Актуальная |
| 2.2.2 Установка ПО, не связанного с исполнением служебных обязанностей | Актуальная |
| 2.2.3 Перехват паролей  или идентификаторов | Актуальная |
| 2.3.1 Утрата ключей и  атрибутов доступа | Актуальная |
| 2.3.2 Непреднамеренная модификация (уничтожение) информации сотрудниками | Актуальная |
| 2.3.4 Выход из строя аппаратно-программных  средств | Актуальная |
| 2.5.1 Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей  информации | Актуальная |
| 2.5.3 Угрозы выявления  паролей по сети | Актуальная |

Защита от **кражи, модификации, уничтожения информации**

Будут сравниваться системы средств защиты информации от несанкционированного доступа (СЗИ от НСД).

Несанкционированный доступ к информации (НСД) – получение защищаемой информации субъектами с нарушением установленных правил управления доступом.

Средства защиты от несанкционированного доступа – программные, технические или программно‐технические средства, предназначенные для предотвращения или существенного затруднения несанкционированного доступа к информации.

КоАП РФ Статья 13.12. Нарушение правил защиты информации. Для граждан: Штраф от 1 500 до 2 500 рублей с конфискацией несертифицированных средств защиты информации или без таковой.

Сравнение СЗИ от НСД:

1. **Система обнаружения и предотвращения вторжений Dallas Lock (СОВ)**

Dallas Lock (СОВ) — сертифицированная гибридная система обнаружения и предотвращения вторжений уровня узла в программном исполнении.

Ключевые особенности:

* Эвристический и сигнатурный анализ попыток нарушения безопасности. Обновление сигнатур сетевых атак и сигнатур анализа журналов операционной системы.
* Защита от атак на сетевые протоколы модели OSI различных уровней.
* Перехват вызова функций операционной системы, гибкая настройка ограничения доступа к системным функциям для недоверенных приложений.
* Гибкая настройка уровня реагирования системы и детализации журналов.

1. **СЗИ Secret Net Studio**

СЗИ Secret Net Studio — комплексное решение для защиты конечных точек. Помимо защиты от НСД продукт включает антивирус, персональный межсетевой экран и модуль авторизации сетевых соединений, систему обнаружения вторжений, а также расширенные средства централизованного управления и мониторинга.

Основные возможности СЗИ Secret Net Studio:

* Защита от НСД обеспечивается механизмами, применяемыми в СЗИ от НСД Secret Net.
* Антивирусная защита — защита от вредоносных исполняемых файлов на рабочих станциях и серверах с возможностью сканирования и запуска заданий по расписанию, а также по требованию администратора или пользователя.
* Межсетевое экранирование — контроль сетевой активности компьютера и фильтрация большого числа протоколов в соответствии с заданными политиками, в том числе на уровне отдельных приложений, пользователей или групп пользователей. Подпись сетевого трафика для защиты от подделки и перехвата внутри локальной сети. Автоматическая генерация правил с их интеллектуальным сложением в режиме обучения межсетевого экрана.
* Защита от сетевых атак (NIPS) — обнаружение атак сигнатурными и эвристическими методами. Автоматическая блокировка атакующих хостов при обнаружении аномальных пакетов, сканировании портов, DoS-атаках и др.
* Шифрование контейнеров — шифрование контейнеров любого размера по алгоритму ГОСТ 28147-89 обеспечивает защиту данных в случае несанкционированного доступа к носителям информации, их утери или кражи. Размещение шифрованных контейнеров на жестком диске или на съемном носителе. Использование аппаратных идентификаторов для хранения ключевой информации.
* Централизованное развертывание, управление и мониторинг. Развертывание обеспечивается централизованной установкой продукта на все рабочие станции контролируемого домена. Настройка сквозных и групповых политик для всех механизмов защиты осуществляется с использованием единого агента безопасности.

**Вывод:**

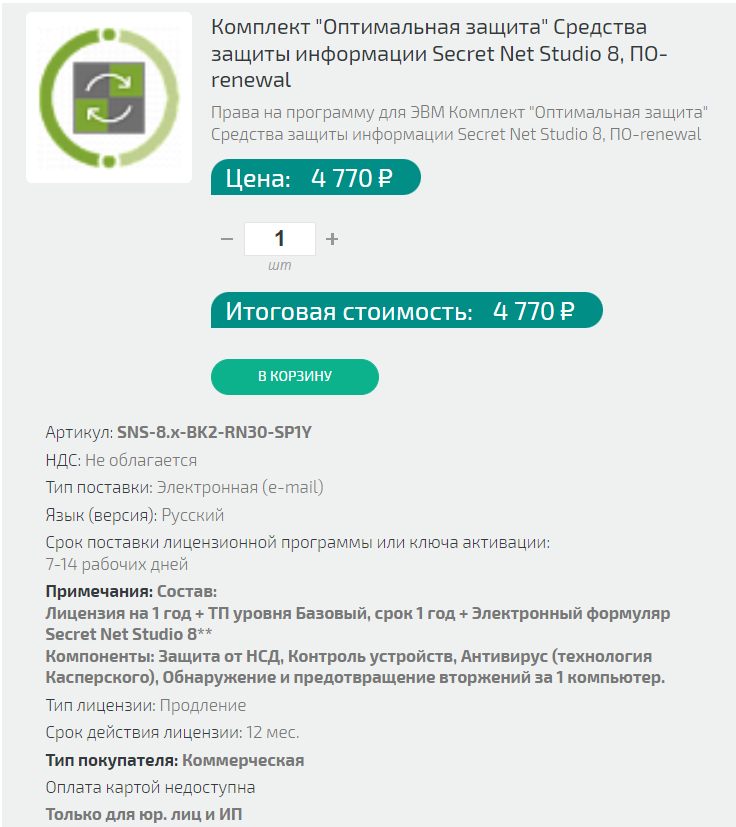
Преимущества SNS:

* САВЗ (средство антивирусной защиты) присутствует только в SNS
* Более расширенный контроль целостности системы
* Более расширенная замкнутая программная среда

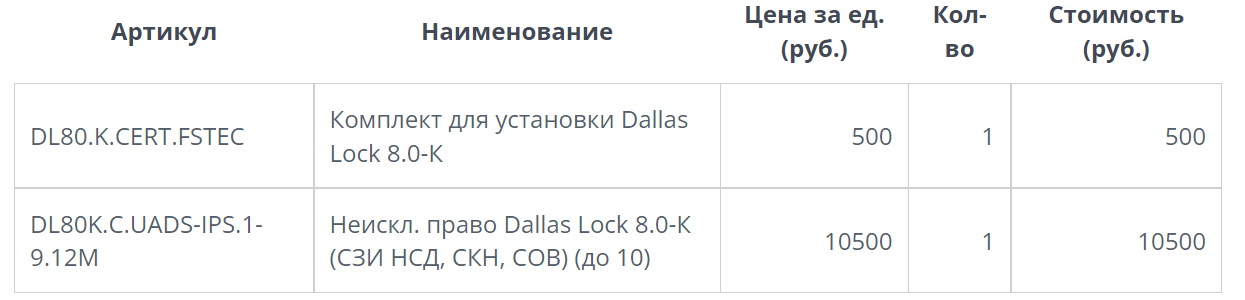
Преимущества Dallas Lock:

* Более расширенная система обнаружения вторжений
* Лучше дискреционное управление доступом
* Отказоустойчивость и восстановление после сбоев
* Межсетевое экранирование

Цена Secret Net Studio:



Цена Dallas Lock:

****

Выбрана была СЗИ Secret Net Studio, т.к.:

* Цена
* Встроенный антивирус
* Защита от сетевых атак, в т.ч. DoS-атак
* Наличие того же межсетевого экрана, что и у более дорогого аналога
* Подробная информация о составе покупаемого продукта