Методические рекомендации к практическому занятию №1

С.А. Краснов

ОБОСНОВАНИЕ И ВЫБОР СЕРТИФИЦИРОВАННЫХ СЗИ ОТ НСД

# МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ К ПРАКТИЧЕСКОМУ ЗАНЯТИЮ № 1

**ОБОСНОВАНИЕ И ВЫБОР СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА (СЗИ ОТ НСД)**

***Цель работы.*** Получить практические навыки по обоснованному выбору СЗИ НСД.

***Постановка задачи.*** Выполнить все шаги работы, необходимые для осуществления обоснованного выбора СЗИ НСД. Результаты зафиксировать в отчете.

***Последовательность действий.***

Шаг 1. Изучить теоретические сведения (материалы) данной практической работы.

Шаг 2. Посетить официальные интернет-ресурсы компаний производителей СЗИ от НСД из перечня таблицы 1, представленного в теоретических сведениях данной практической работы для актуализации состояния дел в области развития СЗИ от НСД данных производителей.

Шаг 3. Сделать качественную оценку способов, методов и механизмов защиты по представленным в таблице 1 СЗИ от НСД с учетом текущего состояния дел.

Шаг 4. Выбрать наиболее важные показатели качества оценки СЗИ от НСД для защищаемой распределенной информационной (автоматизированной) системы (Схему информационной системы предлагается либо разработать самому, либо использовать любую готовую).

Шаг 5. Оценить по выбранным показателям требуемые СЗИ от НСД для Вашей распределенной информационной (автоматизированной) системы с учетом ее структурной схемы.

Шаг 6. Выбрать по результатам оценки наиболее соответствующие сертифицированные СЗИ от НСД для Вашей распределенной информационной (автоматизированной) системы.

Шаг 7. Обосновать сделанный выбор по каждому СЗИ от НСД.

Шаг 8. Всю информацию собрать в единый документ, являющийся отчетом о выборе и обосновании СЗИ НСД для Вашей информационной (автоматизированной) системы.

Вся актуальная информация представлена на официальных интернет-ресурсах компаний и организаций производителей СЗИ от НСД.

***Теоретические сведения.*** Развитие рынка средств защиты от несанкционированного доступа (СЗИ от НСД) в РФ обусловлено необходимостью выполнения требований нормативно правовой базы в области защиты информации (защита ПДН, защита ГИС, защита ГТ).

**Введение:** Значительное количество угроз безопасности информации на рабочих станциях и серверах составляют угрозы несанкционированного доступа (НСД). Они ведут к утечкам конфиденциальных данных и утрате их целостности, что в свою очередь приводит к целому ряду негативных последствий для бизнеса: от репутационного ущерба и финансовых потерь до приостановки бизнес-процессов компании. Кроме того, если компания работает с информацией ограниченного доступа, например, с  персональными данными или государственной тайной, то неизбежно сталкивается с многочисленными требованиями ФСТЭК России и ФСБ России. Невыполнение этих требований приводит к нежелательным санкциям: это могут быть как значительные штрафы, так и полная остановка деятельности компании по требованию регулятора. Для защиты серверов и рабочих станций по требованию регуляторов используются специализированные наложенные средства защиты информации (сокращенно СЗИ от НСД). Сегодня на российском рынке информационной безопасности представлено большое количество СЗИ от НСД для серверов и рабочих станций.

**Что такое СЗИ от НСД:** Российские вендоры включились в процесс разработки решений для защиты автоматизированных рабочих мест и серверов от несанкционированного доступа довольно давно. Первые разработки появились уже начале 90-х для выполнения требований руководящих документов Гостехкомиссии (теперь это ФСТЭК России) по защите информации.

В основном СЗИ от НСД создавались для повышения уровня защищенности операционной системы с использованием механизмов защиты: идентификация и аутентификация пользователей;

дискреционный контроль доступа пользователей;

мандатный контроль доступа пользователей и процессов;

маркировка документов и контроль их вывода на печать;

защита ввода и вывода информации на отчуждаемый физический носитель;

регистрация событий безопасности в журнале событий;

контроль целостности критичных файлов и данных;

контроль доступа к периферийным устройствам и портам ввода-вывода;

гарантированное удаление данных на дисках и выборочное затирание файлов и др.

Требования к этим механизмам защиты описаны в Руководящем документе «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» Гостехкомиссия России, 1992 г.

По типу исполнения СЗИ от НСД бывают программными и программно-аппаратными. К последним относятся комплексы, где помимо специального программного обеспечения для разграничения доступа к ресурсам в составе комплекса есть аппаратный модуль ­ средство доверенной загрузки.

С точки зрения архитектуры СЗИ от НСД могут быть сетевыми и автономными. Сетевые СЗИ от НСД в общем случае включают сервер безопасности, а также агенты защиты, которые устанавливаются на конечные точки — рабочие станции и сервера. Сетевые СЗИ от НСД предусматривают централизованное управление защитными механизмами, а также централизованное получение информации от агентов об изменении состояния защищаемых компьютеров. В автономных СЗИ от НСД защитные механизмы устанавливаются и управляются локально (без привязки к серверу безопасности).

В последнее время наблюдается тенденция создания комплексных решений для защиты рабочих станций и серверов. Причиной этому является желание вендоров выйти из ниши классических СЗИ от НСД на уровень полноценных средств защиты информации на конечных точках (так называемый класс Information-Centric Endpoint Protection). Рецепт комплексных решений заключается в добавлении к классическим СЗИ от НСД модулей сетевой и антивирусной защиты: подсистемы персонального межсетевого экрана, подсистемы обнаружения вторжений уровня хоста, подсистемы антивирусной защиты, поиска уязвимостей, веб-фильтрации и т. д. Управление всеми компонентами осуществляется из единой консоли, что упрощает администрирование СЗИ, а интегрированность защитных механизмов между собой исключает возможность нарушения функционирования защищаемой системы.

**Сертификация СЗИ от НСД на соответствие требованиям ФСТЭК России СЗИ от НСД** должны удовлетворять определенным требованиям руководящих и нормативных документов ФСТЭК России. Если мы говорим о традиционных СЗИ от НСД, которые обеспечивают разграничение доступа пользователей к ресурсам, то такие комплексы должны соответствовать требованиям руководящих документов:

Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» Гостехкомиссия России, 1992 г. (для удобства в статье будем называть ­ РД СВТ).

Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей». Гостехкомиссия России, 1992 г. (для удобства в статье будем называть ­ РД НДВ).

СЗИ от НСД обычно включают и подсистему контроля съемных носителей и сертифицируются на соответствие Требованиям к средствам контроля съемных машинных носителей информации, утвержденные приказом ФСТЭК России от 28 июля 2014 г. № 87.

Кроме того, некоторые программно-аппаратные комплексы помимо разграничения доступа к ресурсам компьютера обеспечивают доверенную загрузку операционной системы — включают модуль доверенной загрузки. Такие СЗИ от НСД дополнительно к приведенным выше требованиям сертифицируются в том числе на соответствие Требованиям к средствам доверенной загрузки, утвержденные приказом ФСТЭК России от 27 сентября 2013 г. № 119.

Комплексные решения, которые помимо разграничения доступа к ресурсам обеспечивают контроль сетевых соединений, защиту от вторжений, а также антивирусную защиту, сертифицируются на соответствие профилей защиты:

Требования к межсетевым экранам, утвержденные приказом ФСТЭК России от 9 февраля 2016 г. № 9).

Требования к системам обнаружения вторжений, утвержденные приказом ФСТЭК России от 6 декабря 2011 г. № 638.

Требования к средствам антивирусной защиты, утвержденные приказом ФСТЭК России от 20 марта 2012 г. № 28.

Российский рынок СЗИ от НСД и основные тенденции его развития Одной из главных причин востребованности сертифицированных СЗИ от НСД на российском рынке является необходимость выполнения требований действующего законодательства и нормативных актов в области защиты информации:

Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Закон Российской Федерации № 5485-I «О государственной тайне» от 21 июля 1993г. и другие.

В настоящее время среди основных игроков рынка сертифицированных СЗИ от НСД можно выделить:

СЗИ от НСД Secret Net, Secret Net Studio и ПАК «Соболь» («Код Безопасности»)

СЗИ от НСД Dallas Lock (компания «Конфидент») СЗИ от НСД «Аккорд» (компания ОКБ САПР)

СЗИ от НСД «Блокхост-сеть К» и «Блокхост-АМДЗ 2.0» («Газинформсервис»)

СЗИ от НСД ПАНЦИРЬ (НПП «Безопасные информационные технологии») СЗИ от НСД Diamond ACS (компания ТСС)

СЗИ от НСД «Страж NT 4.0» (компания «Рубинтех»)

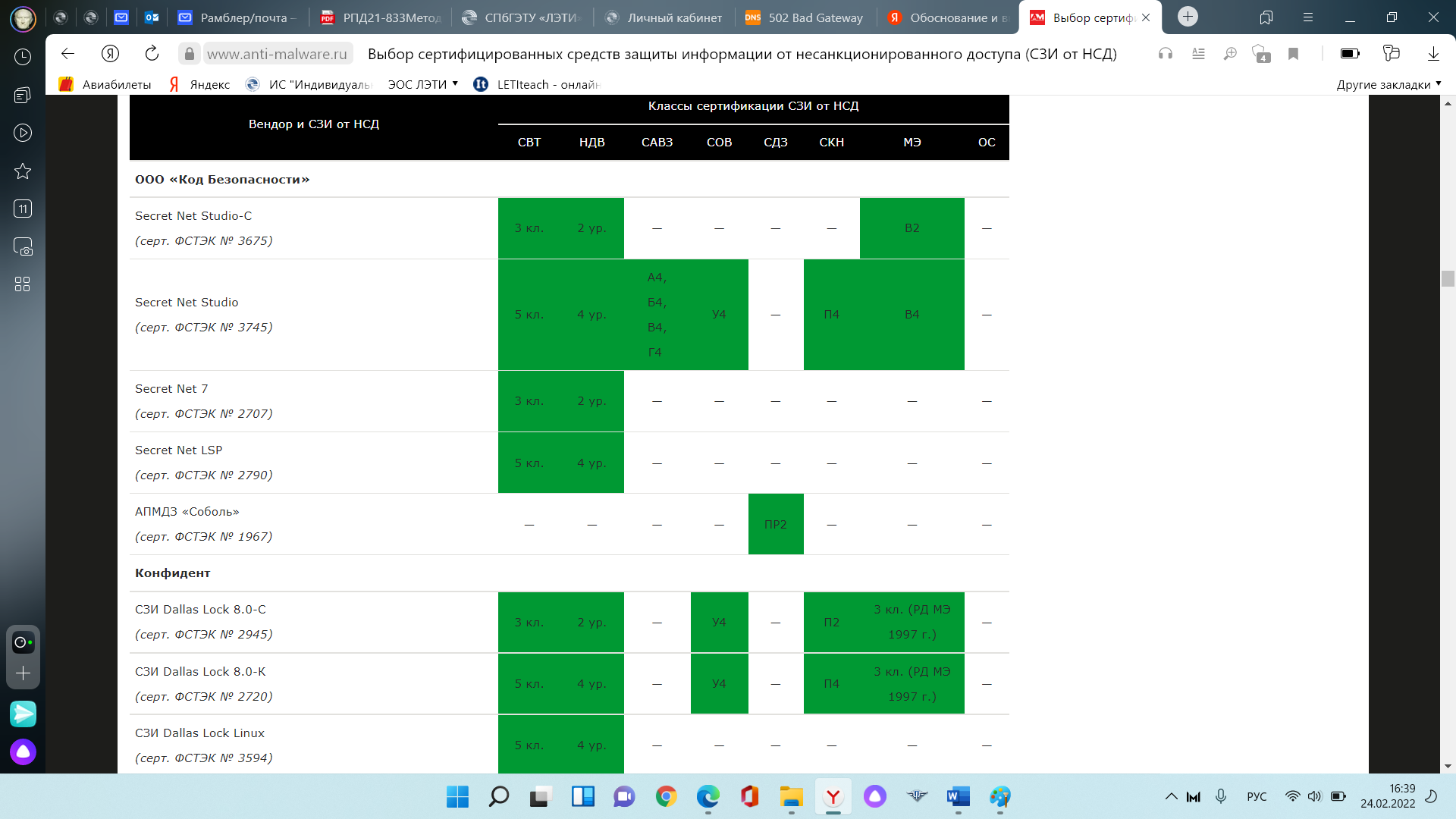
СЗИ от НСД «Аура» (СПИИРАН)

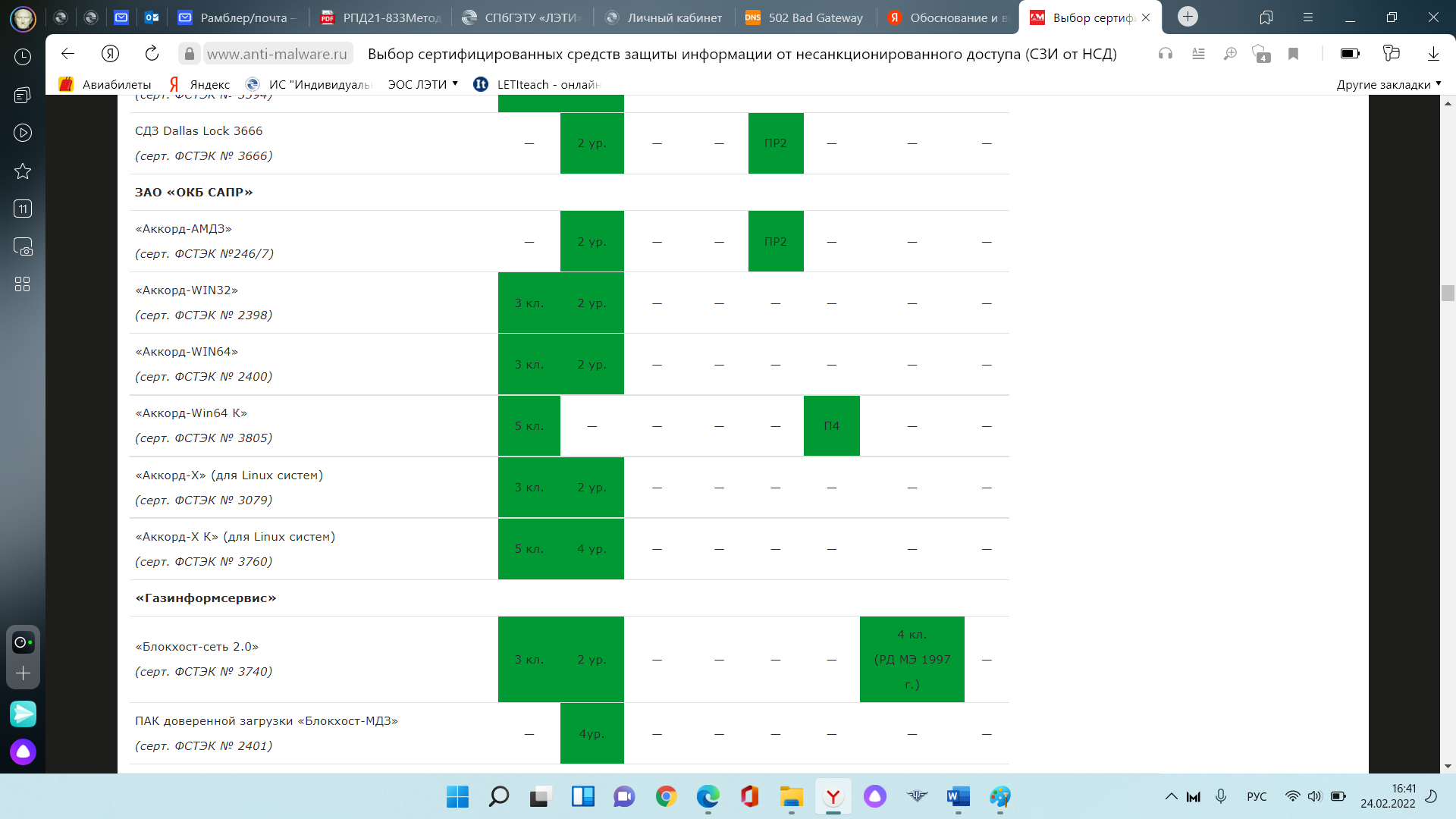
СЗИ от НСД «Фантом» (РНТ)

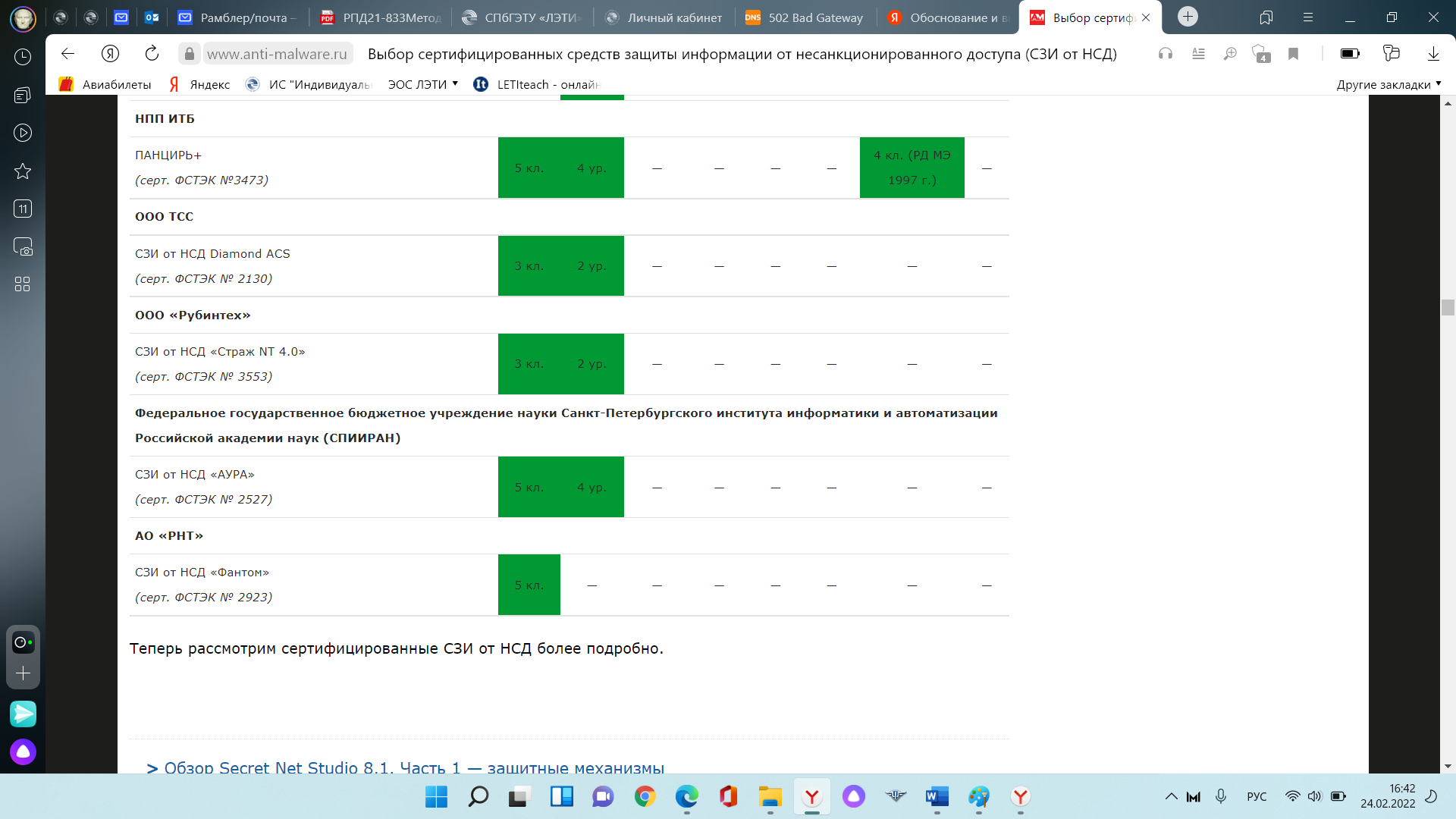
Также на рынке присутствуют некоторые нишевые продукты, например, СРД «КРИПТОН-ЩИТ» (ООО Фирма «Анкад»),СЗИ НСД «Щит-РЖД» (СПИИРАН).

Так как сам рынок СЗИ от НСД возник под влиянием российских регуляторов, то принципиальной характеристикой продукта является не столько широта функциональных возможностей, сколько классы их сертификации ФСТЭК России. Далее в таблице 1 приведем данные по действующим сертификатам наиболее популярных продуктов.

  Таблица 1. Классы сертификации ФСТЭК России популярных СЗИ от НСД







Теперь рассмотрим сертифицированные СЗИ от НСД более подробно.

Обзор основных игроков рынка сертифицированных СЗИ от НСД

## «ГАЗИНФОРМСЕРВИС»

**СЗИ от НСД «Блокхост-Сеть 2.0»**

Средство защиты информации «Блокхост-Сеть 2.0» предназначено для защиты информационных ресурсов от несанкционированного доступа в локальных вычислительных сетях на базе персональных компьютеров, функционирующих под управлением операционных систем Microsoft Windows 2008R2/Vista/7/8/8.1/10/2012/2012R2/2016. «Блокхост-Сеть 2.0» дополняет и усиливает собственные возможности защиты операционной системы, создавая тем самым доверенную рабочую среду функционирования процессов.

СЗИ «Блокхост-Сеть 2.0» состоит из клиентской части СЗИ «Блокхост-Сеть 2.0», в рамках которой реализованы базовые механизмы защиты, и серверной части — сервера безопасности, устанавливаемой на автоматизированное рабочее место администратора безопасности.

СЗИ «Блокхост-Сеть 2.0» выполняет следующие функции защиты: двухфакторная аутентификация пользователей с применением персональных идентификаторов;

дискреционный и мандатный механизмы контроля доступа к информационным ресурсам в соответствии с заданными параметрами безопасности, в том числе по времени;

контроль целостности системного программного обеспечения, прикладного программного обеспечения и информационных ресурсов АРМ;

очистка областей оперативной памяти после завершения работы контролируемых процессов;

гарантированное удаление файлов и папок, что исключает возможность восстановления;

контроль вывода информации на печать и отчуждаемые физические носители, маркировка документов;

контроль запуска процессов; персональный межсетевой экран (контроль доступа к сетевым ресурсам и фильтрация сетевого трафика);

защита от изменения и удаления СЗИ «Блокхост-Сеть 2.0».

**ПАК «Блокхост-МДЗ»**

Программно-аппаратный комплекс «Блокхост-МДЗ» предназначен для решения следующих задач:

двухфакторная аутентификация пользователей для усиления защиты входа на рабочую станцию до загрузки операционной системы;

обеспечение конфиденциальности данных, хранимых на электронных носителях, путем шифрования их содержимого;

контроль целостности файлов с заданной периодичностью;

выполнение гарантированного удаления файлов без возможности их восстановления;

очистка областей оперативной памяти после завершения контролируемых процессов для предотвращения считывания остаточной информации;

сохранение конфиденциальности данных даже при краже или утере носителей;

контроль доступа пользователей к отчуждаемым носителям, оптическим приводам, Wi-Fi и Bluetooth-адаптерам, подключаемым через USB порты.

«Блокхост-МДЗ» состоит из 7 модулей, которые могут быть использованы как единым комплексом, так и по отдельности.

## «КОД БЕЗОПАСНОСТИ»

Компания «Код Безопасности» — российский разработчик программных и аппаратных средств, обеспечивающих защиту информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Компания основана в 2008 году и ведет свою деятельность на основании девяти лицензий ФСТЭК России, ФСБ России и Министерства обороны Российской Федерации. В настоящее время сотрудниками «Кода безопасности» являются более 400 квалифицированных специалистов, многие из которых имеют уникальные компетенции в области разработки ИБ-решений. Свыше 900 авторизованных партнеров компании поставляют ее продукты и обеспечивают их качественную поддержку во всех регионах России и в странах СНГ. Более 32 000 государственных и коммерческих организаций доверяют продуктам «Кода безопасности» и используют их для защиты рабочих станций, серверов, виртуальных инфраструктур, мобильных устройств и сетевого взаимодействия всех компонентов информационных систем.

Для защиты конечных точек компания «Код Безопасности» предлагает несколько решений:

СЗИ от НСД Secret Net — сертифицированное средство защиты информации от несанкционированного доступа для операционных систем семейства MS Windows.

СЗИ от НСД Secret Net LSP — сертифицированное средство защиты информации от несанкционированного доступа для операционных систем семейства Linux.

СЗИ Secret Net Studio — комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования.

АПМДЗ «Соболь» — сертифицированный аппаратно-программный модуль доверенной загрузки.

**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.

**СЗИ от НСД Secret Net LSP**

СЗИ от НСД Secret Net LSP — сертифицированное средство защиты информации от несанкционированного доступа для операционных систем семейства Linux. Возможна интеграция со средствами централизованного управления Secret Net Studio и Secret Net 7, а также совместная работа с терминальным сервером под управлением Windows.

Основные возможности СЗИ от НСД Secret Net LSP:

Защита входа в систему

Разграничение доступа к ресурсам

Разграничение доступа к устройствам

Регистрация событий ИБ

Контроль целостности

Аудит действий пользователей

Затирание остаточной информации

Удобство администрирования благодаря наличию графических и консольных средств управления

Интеграция со средствами централизованного управления Secret Net Studio и Secret Net 7

Включение компьютера в домен Windows

**АПМДЗ «Соболь»**

Электронный замок «Соболь» — это сертифицированный аппаратно-программный модуль доверенной загрузки. ПАК «Соболь» может применяться как устройство, обеспечивающее защиту автономного компьютера, а также рабочей станции или сервера, входящих в состав локальной вычислительной сети. Комплекс имеет широкий выбор форматов исполнения и применяется совместно с продуктами Secret Net 7 и Secret Net Studio как средство, усиливающее механизм обнаружения атак на конечные точки.

Основные возможности ПАК «Соболь»:

Механизм контроля целостности позволяет контролировать неизменность файлов и физических секторов жесткого диска до загрузки операционной системы;

Контроль целостности реестра Windows существенно повышает защищенность рабочих станций от несанкционированных действий внутри операционной системы;

Контроль целостности аппаратной конфигурации компьютера запрещает использование неавторизованных компонентов;

Идентификация и усиленная (двухфакторная) аутентификация пользователей с использование персональных идентификаторов;

Аудит попыток доступа к компьютеру в системном журнале, хранящемся в специальной энергонезависимой памяти;

Блокировка несанкционированной загрузки операционной системы со съемных носителей не дает злоумышленнику возможность обойти СЗИ, работающие «внутри» ОС;

Сбор и хранение данных о событиях безопасности облегчает расследование инцидентов;

Использование сторожевого таймера обеспечивает блокировку компьютера в нештатной ситуации — если после включения компьютера и по истечении заданного интервала времени управление не передано комплексу «Соболь»;

Применение аппаратного датчика случайных чисел, соответствующего требованиям ФСБ, обеспечивает повышенный класс защиты СКЗИ.

## «КОНФИДЕНТ»

Продуктовая линейка Dallas Lock Центра защиты информации компании «Конфидент» представлена современными средствами защиты информации для платформ Windows и Linux. Решения компании позволяют не только привести информационные системы в соответствие требованиям законодательства, но и создать их комплексную защиту благодаря таким уникальным возможностям, как наличие элементов функциональности DLP-систем, управления привилегированными пользователями, создание доверенной рабочей среды.

**СЗИ Dallas Lock 8.0**

СЗИ Dallas Lock 8.0 —сертифицированная система защиты информации накладного типа для автономных и сетевых АРМ (применима для сложных сетевых инфраструктур). Предназначена для защиты конфиденциальной информации (редакции «К» и «С»), в том числе содержащейся в автоматизированных системах до класса защищенности 1Г включительно, в государственных информационных системах до 1 класса защищенности включительно, в информационных системах персональных данных для обеспечения 1 уровня защищенности персональных данных, в автоматизированных системах управления производственными и технологическими процессами до 1 класса защищенности включительно, а также для защиты информации, содержащей сведения, составляющие государственную тайну (редакция «С») до уровня «совершенно секретно» включительно.

Ключевые особенности:

Собственные сертифицированные механизмы управления информационной безопасностью, дублирующие (подменяющие) стандартные механизмы Windows.

Возможность применения в различных версиях и редакциях Windows (от Windows XP до Windows 10) на персональных, портативных компьютерах (ноутбуках, планшетах), серверах, в виртуализированных средах.

Широкий набор дополнительных возможностей.

Наличие модуля СКН — это сертифицированное средство контроля съемных машинных носителей информации (по Требованиям ФСТЭК России к СКН).

Бесшовная интеграция с другими решениями продуктовой линейки Dallas Lock.

Совместимость с ИТ- и ИБ-решениями других производителей.

**Межсетевой экран Dallas Lock (МЭ)**

Межсетевой экран Dallas Lock (МЭ) — сертифицированный модуль СЗИ НСД Dallas Lock 8.0, выполняющий функции персонального межсетевого экрана с централизованным управлением, аудитом событий информационной безопасности и предназначенный для защиты рабочих станций и серверов от несанкционированного доступа по сети. МЭ осуществляет контроль и фильтрацию проходящих через интерфейсы компьютера сетевых пакетов в соответствии с заданными правилами, блокирует нежелательную сетевую активность и уведомляет о попытках нарушения заданных правил. Модуль тесно интегрирован с СЗИ НСД Dallas Lock 8.0, что позволяет производить централизованное развертывание и настройку функциональности НСД и МЭ из единого общего интерфейса.

Ключевые особенности:

Защита конфиденциальной информации в сетях, подключенных к сетям общего пользования.

Интеграция с СЗИ Dallas Lock 8.0.

Гибкая настройка правил фильтрации в соответствии с сетевой моделью OSI всех уровней.

**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.

**Средство доверенной загрузки Dallas Lock (СДЗ)**

Dallas Lock (СДЗ) — сертифицированное средство доверенной загрузки уровня платы расширения, предназначенное для защиты информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно, а также для защиты конфиденциальной информации, в том числе содержащейся в государственных информационных системах, информационных системах персональных данных.

Ключевые особенности:

Полноценная поддержка интерфейса UEFI.

Разъемы для подключения: PCI (через переходник), PCI-Express, Mini PCI-Express, M.2.

Полное администрирование СДЗ без использования ресурсов загружаемой штатной операционной системы.

Установка дополнительных программных модулей (агентов) в среду штатной операционной системы не требуется.

Возможность подключения датчика вскрытия корпуса на плате PCI Express.

Унифицированный с другими продуктами Dallas Lock дизайн интерфейса СДЗ.

Централизованное управление (функциональность будет доступна в рамках планового обновления).

**СЗИ НСД Dallas Lock Linux**

Dallas Lock Linux — сертифицированная СЗИ от НСД накладного типа для рабочих мест и серверов под управлением операционных систем семейства Linux. Не так давно мы обозревали СЗИ НСД Dallas Lock Linux на нашем сайте.

Ключевые особенности СЗИ НСД Dallas Lock Linux:

Поддерживает широкий набор современных дистрибутивов Linux.

Консоль удаленного управления СЗИ из Windows и Linux.

Сервис-ориентированная архитектура.

Современный графический интерфейс (GUI).

Универсальная лицензия.

## НПП ИТБ

Научно-производственное предприятие «Информационные технологии в бизнесе» для защиты автоматизированных рабочих мест и серверов предлагает Комплексную систему защиты информации «Панцирь+».

**КСЗИ «Панцирь+»**

Это сертифицированная ФСТЭК России комплексная система защиты информации от несанкционированного доступа, имеющая в своем составе сетевой экран. Комплекс предназначен для защиты операционных систем семейства Microsoft Windows. В части защиты от целевых атак КСЗИ «Панцирь+» — это система защиты класса Last frontier — образует последний рубеж эшелонированной защиты информации. В задачи КСЗИ «Панцирь+» входит снижение рисков потерь от реализации атак, в предположении о том, что соответствующие угрозы не смогут быть выявлены на ранних стадиях обнаружения и атаки будут осуществлены.

В КСЗИ «Панцирь+» реализованы следующие три основные группы механизмов защиты:

механизмы контроля и разграничения прав доступа субъектов к статичным объектам — к объектам, присутствующим в системе на момент назначения прав доступа к ним субъектов администратором. К таким объектам относятся локальные и разделенные в сети файловые объекты, объекты реестра операционной системы, файловые накопители, определяемые их идентификаторами с учетом серийных номеров, сетевые объекты, локальные и сетевые принтеры и т. д. Этими механизмами реализуется разграничительная политика доступа субъектов к объектам;

механизмы контроля и разграничения прав доступа субъектов к создаваемым объектам — к объектам, отсутствующим в системе на момент назначения прав доступа субъектов к объектам администратором, создаваемым пользователями впоследствии. К таким объектам относятся создаваемые файлы и данные, временно хранящиеся в буфере обмена. Такими механизмами реализуется разделительная политика между субъектами доступа;

механизмы защиты от обхода разграничительной и разделительной политик доступа. Эти механизмы также реализуют контроль доступа, но уже применительно к системным объектам операционной системы — к сервисам олицетворения, к возможностям прямого доступа к дискам и инжектирования кода в процессы, к переменным BIOS UEFI (NV RAM) и загрузчику ОС и т. д.

Принципиальной особенностью реализации механизмов защиты является назначение прав доступа субъектам, к объектам, а не к объектам субъектов, как в иных средствах защиты. Это позволяет использовать при задании правил доступа для идентификации объектов масок и переменных среды окружения, что не только существенно упрощает задачу администрирования, но делает возможным тиражирование настроек при внедрении комплекса.

Все механизмы защиты из состава КСЗИ «Панцирь+» сертифицированы на соответствие РД СВТ, РД МЭ, на отсутствие НДВ, большая часть ключевых механизмов защиты, в том числе от целевых атак, сертифицировано на соответствие ТУ, что обеспечивает их легитимное использование в соответствующих информационных системах: КИИ, ГИС, ИСПДн, АСУ ТП, в ИС цифровой экономики РФ.

## ОКБ САПР

ОКБ САПР — компания-разработчик программно-аппаратных средств защиты информации от несанкционированного доступа, в том числе криптографических, с более чем двадцатилетним стажем (год основания — 1989).

Продуктовая линейка «Аккорд» компании ОКБ САПР представлена программно-аппаратными комплексами для защиты Windows и Linux рабочих мест и серверов, которая включает:

«Аккорд-АМДЗ» — аппаратный модуль доверенной загрузки. Программно-аппаратные комплексы «Аккорд-Win32», «Аккорд-Win64» — для разграничения доступа пользователей к рабочим станциям и серверам, работающим под управлением 32- и 64-разрядных Windows.

Программно-аппаратные комплексы Аккорд-Х, Аккорд-Х К — для разграничения доступа пользователей к рабочим станциям и серверам под управлением Linux.

СУЦУ — система удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд». Отметим, что в основе всех решений семейства «Аккорд» лежит концепция аппаратной защиты, которую коротко можно сформулировать как необходимость наличия резидентного аппаратного компонента компьютерной системы, обеспечивающего ее защиту от НСД.

**«Аккорд-АМДЗ»**

СЗИ НСД «Аккорд-АМДЗ» представляет собой аппаратный модуль доверенной загрузки (плата расширения, устанавливаемая в свободный слот материнской платы) для серверов и рабочих станций локальной сети.

Комплекс обеспечивает доверенную загрузку различных операционных систем — загрузку только с заранее определенных постоянных носителей (например, только с жесткого диска) после успешного завершения специальных процедур: проверки целостности технических и программных средств компьютера (с использованием механизма пошагового контроля целостности) и идентификации/аутентификации пользователя.

**ПАК «Аккорд-Win32» (TSE), ПАК «Аккорд-Win64» (TSE) и «Аккорд-Win64 К»**

Комплексы «Аккорд-Win32», «Аккорд-Win64» и «Аккорд-Win64 К» предназначены для разграничения доступа пользователей к рабочим станциям, терминалам и терминальным серверам под управлением операционных систем семейства Windows.

Комплексы «Аккорд-Win32» и «Аккорд-Win64» реализованы с аппаратным модулем «Аккорд-АМДЗ» (входит в состав продукта). «Аккорд-Win64 К» реализован программно.

Возможности:

Идентификация/аутентификация пользователей.

Аппаратный контроль целостности системных файлов и критичных разделов реестра.

Доверенная загрузка операционной системы (реализуется ПАК «Аккорд-АМДЗ», входит в состав продуктов «Аккорд-Win32» (TSE) и ПАК «Аккорд-Win64» (TSE)).

Контроль целостности программ и данных, их защита от несанкционированных модификаций.

Создание индивидуальной для каждого пользователя изолированной рабочей программной среды.

Разграничение доступа пользователей к массивам данных и программам с помощью дискреционного контроля доступа.

Разграничение доступа пользователей и процессов к массивам данных с помощью мандатного контроля доступа.

Автоматическое ведение протокола регистрируемых событий в энергонезависимой памяти аппаратной части комплекса.

Усиленная аутентификация терминальных станций с помощью контроллера «Аккорд» или ПСКЗИ ШИПКА.

Идентификация/аутентификация пользователей, подключающихся к терминальному серверу (с использованием ТМ-идентификатора или ПСКЗИ ШИПКА).

Управление терминальными сессиями. Контроль печати на принтерах.

Контроль доступа к USB-устройствам.

**СУЦУ СЗИ** **от НСД**

СУЦУ — система удаленного централизованного управления средствами защиты информации от несанкционированного доступа «Аккорд» обеспечивает централизованный мониторинг событий информационной безопасности и управления средствами защиты информации от несанкционированного доступа.

Основные возможности СУЦУ:

Управление подконтрольными рабочими станциями и серверами.

Управление пользователями.

Централизованный сбор и хранение информации о зарегистрированных событиях доступа к подконтрольным объектам.

Централизованное управление средствами защиты информации от несанкционированного доступа на подконтрольных объектах.

Управление доступом к коммутационным портам и периферийным устройствам.

**СЗИ от НСД «Аккорд-X»**

Программно-аппаратный комплекс средств защиты информации «Аккорд-X» предназначен для разграничения доступа пользователей к рабочим станциям под управлением Linux.

Комплекс «Аккорд-X» реализован с аппаратным модулем «Аккорд-АМДЗ» (входит в состав продукта). «Аккорд-X К» реализован программно.

Основные возможности «Аккорд-X»:

Защита от несанкционированного доступа к компьютерам (включая возможность ограничения разрешенных часов работы каждого пользователя).

Идентификация/аутентификация пользователей.

Аппаратный контроль целостности системных файлов.

Доверенная загрузка операционной системы.

Статический и динамический контроль целостности данных, их защита от несанкционированных модификаций.

Разграничение доступа пользователей, процессов к массивам данных (объектам) с помощью дискреционного контроля доступа.

Разграничение доступа пользователей, процессов к массивам данных (объектам) с помощью мандатного контроля доступа.

Разграничение доступа пользователей к определенным процессам. Контроль доступа к периферийным устройствам.

Создание индивидуальной для каждого пользователя изолированной рабочей программной среды.

Автоматическое ведение протокола регистрируемых событий.

Контроль печати на локальных и сетевых принтерах, протоколирование вывода данных на печать, маркировка распечатанных данных (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

## РНТ

**СЗИ от НСД «Фантом»**

Это программное средство, предназначенное для создания защищенного рабочего места и серверного решения с использованием технологий виртуализации. «Фантом» позволяет обрабатывать информацию различного уровня конфиденциальности на одной аппаратной единице. Исполнение ПАК «Фантом» на внешнем жестком диске благодаря защите от НСД носителя, каналов связи, а также наличию дополнительных средств защиты позволяет выездным сотрудникам использовать произвольную аппаратную единицу (ноутбук, стационарный компьютер и т. п.) и работать с конфиденциальной информацией в условиях небезопасной среды (в заграничных командировках, в гостиницах, дома и т. п.).

СЗИ от НСД «Фантом» решает следующие основные задачи:

Безопасная работа на любом компьютере (коллективного пользования, домашний) с индивидуального переносного USB-диска.

Контроль операционной системы с использованием аппаратных технологий виртуализации.

Контроль периферийных устройств компьютера, включая встроенную память и диск, с уровня гипервизора.

Прозрачное функционирование для пользователя.

Надежная реализация криптографических функций на уровне гипервизора.

Повышенная отказоустойчивость за счет механизма снимков состояния и хранилища резервных копий.

Аудит происходящих событий.

Контроль сетевого взаимодействия.

Усиленная аутентификация пользователей.

Возможность отдельного размещения нескольких рабочих мест на одном компьютере или на внешнем загружаемом USB-диске.

Возможность работы исключительно с индивидуального переносного внешнего USB-диска.

Полная изоляция рабочих мест (виртуальных доменов).

Контроль работы вычислительных ресурсов в режиме реального времени.

Поддержка криптографических функций по требованиям безопасности.

Наличие механизма хранения резервных копий, что позволяет в случае внештатной ситуации (сбой в случае воздействия злоумышленника, некорректно работающего программного обеспечения и т. п.) в любое время вернуться к сохраненному состоянию системы или ее отдельных компонентов.

Защита от изменения системных компонент ВМ.

Контроль целостности операционной системы, окружения пользователя и отдельных компонентов с целью противостоять проникновению в среду вредоносного кода.

В СЗИ «Фантом» также есть встроенные МСЭ, антивирус (проверяются все файлы, которые пользователь переносит из одной ВМ в другую) (данная функциональность не сертифицирована), система для отображения и анализа журнальных записей. Также можно отметить наличие VPN-клиента на уровне самого продукта, а не отдельных ВМ. Кроме того, возможна интеграция комплекса с системой обнаружения компьютерных атак «ФОРПОСТ».

## РУБИНТЕХ

**СЗИ от НСД «Страж NТ версия 4.0»**

Компания «Рубинтех» для защиты автоматизированных рабочих мест и серверов предлагает решение «Страж NT 4.0». СЗИ от НСД «Страж NТ версия 4.0» представляет собой программный комплекс средств защиты информации с использованием электронных идентификаторов и предназначена для защиты информационных ресурсов от несанкционированного доступа:

на автономных рабочих станциях;

рабочих станциях в составе рабочей группы или домена локальной вычислительной сети;

серверах (в том числе и терминальных).

«Страж NТ 4.0» может применяться при разработке систем защиты информации для многопользовательских автоматизированных систем (АС),  информационных систем персональных данных (ИСПДн) и государственных информационных систем (ГИС)  в соответствии с требованиями законодательства Российской Федерации.

Функционирует в среде 32- и 64-разрядных операционных систем Microsoft Windows.

Сертифицирован ФСТЭК России на соответствие РД СВТ по 3-му классу защищенности и РД НДВ по 2-му уровню контроля НДВ.

Ключевые особенности СЗИ от НСД «Страж NT версия 4.0»:

Возможность сетевого развертывания и настройки и СЗИ с любого рабочего места в сети.

Децентрализованное управление без сервера безопасности.

Поддержка компьютеров c UEFI и GPT-разбиением диска.

Сокрытие логической структуры загрузочного жесткого диска.

Наличие гибкого механизма сценариев настроек.

Реализация дискреционного и мандатного принципов разграничения доступа, в том числе и на съемных носителях информации.

Возможность одновременной работы с документами разных грифов в одном сеансе (без смены сеанса пользователя).

Режим виртуализации объектов при настройке мандатной защиты.

Поддержка терминальных сессий.

Основные функциональные возможности СЗИ от НСД «Страж NT 4.0»:

Двухфакторная аутентификация до загрузки операционной системы (в том числе и для виртуальной среды) с использованием аппаратных идентификаторов.

Дискреционный принцип контроля доступа к ресурсам системы.

Мандатный принцип контроля доступа к ресурсам системы.

Создание замкнутой программной среды пользователя, позволяющей ему запуск только разрешенных приложений.

Регистрация событий безопасности, в том числе и действий администратора.

Маркировка выдаваемых на печать документов независимо от печатающего их приложения.

Гарантированная очистка освобождаемой оперативной памяти, содержимого защищаемых файлов при их удалении, файлов подкачки при завершении работы системы.

Контроль целостности защищаемых ресурсов системы и компонентов системы защиты информации.

Управление пользователями.

Управление носителями информации.

Управление устройствами.

Преобразование информации на отчуждаемых носителях.

Тестирование системы защиты информации.

## СПИИРАН НИО ПИБ

Санкт-Петербургского института информатики и автоматизации Российской академии наук (СПИИРАН) для защиты от НСД серверов и рабочих станций предлагает СЗИ «Аура».

**СЗИ «Аура»**

Решение предназначено для комплексной защиты информации, обрабатываемой на ПЭВМ под управлением Microsoft Windows.

СЗИ от НСД «Аура» решает следующие основные задачи:

обеспечение доверенной среды для аутентификации пользователей и контроля целостности информационных объектов;

усиленная аутентификация; многоуровневый контроль целостности информационных объектов вычислительной системы;

контроль доступа к устройствам, файлам и папкам; управление печатью, автоматическая маркировка и учет документов;

достоверное уничтожение информационных объектов;

регистрация действий пользователя в системных журналах;

идентификация и аутентификация пользователей в доверенной среде с применением электронных устройств Rutoken.

## ТСС

Компания ТСС для защиты автоматизированных рабочих мест и серверов предлагает программно-аппаратный комплекс Diamond ACS.

**Diamond ACS**

Это кроссплатформенный программно-аппаратный комплекс средств защиты информации от несанкционированного доступа. Продукт позволяет осуществлять доверенную загрузку и физическое разделение контуров различной степени конфиденциальности на автоматизированных рабочих местах. Diamond ACS может быть реализован в автономной или сетевой версиях в программном и программно-аппаратном видах (с подключением аппаратного замка Diamond ACS HW).

Основные функции Diamond ACS в программно-аппаратном исполнении:

централизованное управление (единая консоль управления политиками безопасности);

контроль целостности загрузочного сектора жесткого диска до загрузки операционной системы (опционально);

возможность работы в двух изолированных контурах различного уровня конфиденциальности на одной машине (опционально);

разграничение доступа пользователей к данным, устройствам и приложениям на основе дискреционного и мандатного принципов контроля доступа;

статический и динамический контроль целостности приложений и данных;

автоматическая регистрация системных событий в журналах безопасности;

контроль вывода на печать и маркировка документов, содержащих конфиденциальную информацию;

блокировка рабочего места по периоду неактивности;

возможность настройки расписания доступа пользователя в систему;

функция многофакторной аутентификации с использованием биометрических данных пользователя (вход в систему по отпечаткам пальцев, смарт-карте и пин-коду).

Diamond ACS поддерживает Windows и Linux. Diamond ACS также может применяться в системах терминального доступа, построенных на базе терминальных служб Microsoft RDS и программного обеспечения Citrix (функционирующего на базе протокола ICA).

Комплекс обеспечивает возможность совместной работы со следующими СЗИ и СКЗИ:

по части обеспечения безопасного межсетевого взаимодействия и обнаружения вторжений — Diamond VPN/FW

для хранения ключевой и идентифицирующей информации — JaCarta (производства ЗАО «Аладдин Р.Д.»).

**Выводы** Вы рассмотрели российский рынок сертифицированных средств защиты информации от несанкционированного доступа для конечных точек, Вы узнали, каким требованиям должны соответствовать СЗИ от НСД, а также обозначили основных игроков российского рынка СЗИ от НСД.

Основным драйвером рынка сертифицированных СЗИ от НСД является необходимость выполнения требований действующего законодательства и нормативных актов в области защиты информации (защита ПДН, защита ГИС, защита ГТ). Хотя изначально СЗИ от НСД создавались применительно к решению задач усиления встроенных в операционные системы механизмов защиты, современные продукты этого класса эволюционируют в сторону комплексной защиты конечных точек сети от внешних и внутренних угроз, где функциональность СЗИ от НСД является лишь одной из составляющих.

К наиболее популярным в России продуктам можно отнести Secret Net Studio, «Аккорд», Dallas Lock, «Блокхост-сеть», Diamond ACS, «Панцирь», «Страж NT», «Аура» и «Фантом». Среди комплексных решений для защиты автоматизированных рабочих мест и серверов можно выделить продукты Dallas Lock ЦЗИ «Конфидент» и Secret Net Studio компании «Код Безопасности». Помимо стандартных функций СЗИ от НСД у этих решений есть персональный межсетевой экран, система обнаружения вторжений. Secret Net Studio включает антивирусный модуль на базе антивирусного ядра ESET, а также планируется интеграция с Kaspersky Anti-Virus.

***Контрольные вопросы***

1. ***Опишите процесс построения системы информационно-компьютерной безопасности?***
2. ***Перечислите основные руководящие документы ФСТЭК по классификации АС, средств вычислительной техники (СВТ), межсетевых экранов (МЭ) и программного обеспечения (ПО)?***
3. ***Что включает в себя модель CIA?***
4. ***Сколько классов защищенности АС от НСД определено в РД, охарактеризуйте их***
5. ***Перечислите основные виды преднамеренных угроз:***
6. ***Что относиться к угрозам безопасности сетевого взаимодействия:***
7. ***Что относиться к угрозам несанкционированного использования компьютерных ресурсов:***
8. ***К мерам по предупреждению несанкционированного воздействия на компьютерные ресурсы относятся:***
9. ***Средства защиты информации – это…***
10. ***Функциональные требования к АСЗИ включают следующие группы требований:***
11. ***Система защиты АСЗИ должна выполнять следующие функции:***
12. ***Основными функциями СРД являются:***
13. ***Какие функции выполняют обеспечивающие средства для СРД:***
14. ***Разграничение доступа – это…, Авторизация – это…***
15. ***Контроль целостности программного и информационного окружения***
16. ***В чем суть криптографической защиты хранящейся информации.***
17. ***Какими важными достоинствами обладает Secret Net?***
18. ***Перечислите типы МЭ?***
19. ***Опишите назначение и возможности системы защиты Dallas Lock.***

***Дополнительные материалы, информационные источники***

1. Сайт компании ”Код Безопасности” https://www.securitycode.ru/
2. Сайт компании ”Конфидент” https://dallaslock.ru/
3. Сайт компании «Лаборатория Касперского» <https://www.kaspersky.ru/>
4. Сайт компании ГК Astra Linux <https://astralinux.ru/>
5. Сайт компании «Доктор Веб» <https://www.drweb.ru/>

**Методика текущего контроля**

Текущий контроль включает в себя контроль посещаемости (не менее 80 % занятий), сдача 4 коллоквиумов по тематике дисциплины (проверка знаний и умений по каждой теме) по результатам которого студент получает допуск на экзамен. На коллоквиумах проводится защиты работ, которые проводились на практических занятиях.  В ходе проведения практических занятий целесообразно привлечение студентов к как можно более активному участию в дискуссиях, решении задач, обсуждениях и т. д. При этом активность студентов также может учитываться преподавателем, как один из способов текущего контроля на практических занятиях.  самостоятельной работы студентов

Изучение дисциплины сопровождается **самостоятельной работой студентов (СРС)** с рекомендованными преподавателем литературными источниками и информационными ресурсами сети Интернет. Планирование времени для изучения дисциплины осуществляется на весь период обучения, предусматривая при этом регулярное повторение пройденного материала. Обучающимся, в рамках внеаудиторной самостоятельной работы, необходимо регулярно дополнять сведениями из литературных источников материал, законспектированный на лекциях. При этом на основе изучения рекомендованной литературы целесообразно составить конспект основных положений, терминов и определений, необходимых для освоения разделов учебной дисциплины. Особое место уделяется консультированию, как одной из форм обучения и контроля самостоятельной работы. Консультирование предполагает особым образом организованное взаимодействие между преподавателем и студентами, при этом предполагается, что консультант либо знает готовое решение, которое он может предписать консультируемому, либо он владеет способами деятельности, которые указывают путь решения проблемы.

**Текущая СРС по ПЗ №1 состоит из:**

1. Работа с лекционным материалом, с учебной литературой - 2 ак.ч;
2. Опережающая самостоятельная работа (изучение нового материала до его изложения на занятиях) 1 ак.ч.
3. Самостоятельное изучение разделов дисциплины - 1,5 ак.ч.
4. Подготовка к лабораторным работам, к практическим и семинарским занятиям - 2,5 ак.ч
5. Подготовка к контрольным работам, коллоквиумам - 1,5 ак.ч.

Контроль самостоятельной работы студентов осуществляется на лекционных и практических занятиях студентов по методике, описанной выше.

Доцент кафедры ИБ

Краснов С.А.