**Министерство образования и науки Российской Федерации**

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«Владимирский государственный университет**

**имени Александра Григорьевича и Николая Григорьевича Столетовых»**

**(ВлГУ)**

Институт информационных технологий и радиоэлектроники

Кафедра информатики и защиты информации\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

***Методические рекомендации для специалистов по проведению лабораторных занятий***

**7 семестр**

**«Программно-аппаратные средства защиты информации»**

Специальность 10.05.04 «Информационно-аналитические системы безопасности»\_\_\_

Специализация «Автоматизация информационно-аналитической деятельности»\_\_\_\_\_

Уровень высшего образования \_\_\_\_\_\_\_\_специалитет\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Форма обучения \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_очная\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Владимир 2021**

Содержание

**Лабораторная работа 1.** Разработка ПО разграничения полномочий пользователей

**Лабораторная работа 2.** Защита программного обеспечения от изменения и копирования.

**Лабораторная работа 3.** Разработка и программная реализация криптографических алгоритмов.

**Лабораторная работа 4.** Изучение способов формирования электронной цифровой подписи (ЭЦП) на основе КриптоПро CSP 3.9 R2 / КриптоПро CSP 4.0 - для Windows 10

**Лабораторная работа 5.** Изучение способов формирования электронной цифровой подписи (ЭЦП) на основе ViPNet CSP 4.2 - для Windows 10

**Лабораторная работа 6.** Организация защищенного обмена информацией на основе использования программы PGP

**Лабораторная работа 7.** Организация защищенного канала с помощью VPN

**Лабораторная работа 8.** Программная реализация защиты программ с помощью электронных ключей типа «HASP HL Pro»

# ПРАВИЛА ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Главное назначение лабораторных занятий – приобретение студентами необходимых умений и навыков в установке, настройке и использовании специализированного программного и аппаратного обеспечения.

Студенты выполняют лабораторные работы по графику.

Каждому занятию предшествует предварительная подготовка студента, которая включает в себя:

а) ознакомление с содержанием лабораторной работы;

б) проработку теоретической части (описание программных и аппаратных средств, процесс установки и настройки, перечень необходимого предустановленного ПО);

в) составление бланка отчета по лабораторной работе в соответствии с принятыми стандартами.

Отчет выполняется на листах стандартного размера 297×210 мм (формат А4). Записи на оборотной стороне листа не допускаются.

Отчет должен содержать:

1) название лабораторной работы;

2) цель;

3) задачу;

4) теоретическую часть;

5) описание метода решения поставленной задачи;

6) заключение.

Теоретическая часть должна быть краткой, занимать не более листа и содержать общие сведения об использованном программном или аппаратном обеспечении.

Студент должен помнить, что методические указания к лабораторным работам являются только основой для их выполнения. Теоретическую подготовку к каждой лабораторной работе необходимо осуществлять с помощью дополнительной литературы (учебной литературы).

К выполнению новой (следующей) работы допускаются студенты, сдавшие отчет по предыдущей лабораторной работе. Формальным признаком готовности студента к занятию является наличие у него предустановленного ПО по предстоящей работе.

Студенты, получившие допуск, приступают к выполнению лабораторной работы. В лаборатории необходимо строго соблюдать правила техники безопасности. В ходе занятия запрещается заниматься посторонними делами и мешать выполнению работ студентами.

Отчет у каждого студента должен быть индивидуальным. Не сделанные без уважительной причины работы выполняются с разрешения преподавателя в специально отведенное время.

В конце занятия полностью оформленный отчет по лабораторной работе сдается преподавателю. Возможно оформления отчета дома.

Защита лабораторной работы проводится на следующем занятии и включает в себя такие элементы, как:

а) собеседование по работе (демонстрация результатов);

б) обсуждение результатов выполнения работы.

Результатом прохождения каждого элемента является оценка, выставляемая по шкале зачтено/незачтено. Баллы за лабораторную работу выставляются при наличии зачетов по всем этапам приема работы. Возможны ситуации, когда на лабораторном занятии студенты работают по темам, которые еще не освещались в лекциях и не изучались на практических занятиях. В связи с этим важна и ответственна роль учебников, учебных пособий и справочной литературы, которые должны иметь студенты на занятиях. В данном случае дополнительные учебные материалы выдаются преподавателем на лабораторном занятии.

По окончании занятия студенты приводят в порядок рабочие места, а принадлежности к лабораторной работе сдают лаборанту.

# Описание лабораторных работ

## ЛАБОРАТОРНАЯ РАБОТА 1. РАЗРАБОТКА ПО РАЗГРАНИЧЕНИЯ ПОЛНОМОЧИЙ ПОЛЬЗОВАТЕЛЕЙ

**Цели работы**

* Изучение принципов разработки ПО разграничения полномочий пользователей.
* Исследование механизмов работы с реестром ОС MS Windows.
* Изучение принципов работы с сертификатами.
* Изучение принципов защиты ПО.

**Выполнение работы:**общая часть + индивидуальное задание для подгруппы. Язык программирования выбирается произвольно, защищаемый объект выбирается произвольно. Защищаемым объектом может быть разрабатываемая программа - разграничивается доступ к ее функциям.

**Введение**

Разрабатываемая программа предназначена для повышения уровня защищенности системы путем ограничения доступа пользователей к системе. Программа должна обеспечивать работу в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя.

В режиме администратора программа должна поддерживать следующие функции (при правильном вводе пароля):

* смена пароля администратора (при правильном вводе старого пароля);
* просмотр списка имен зарегистрированных пользователей и установленных для них параметров (блокировка учетной записи, включение ограничений на выбираемые пароли) – всего списка целиком в одном окне или по одному элементу списка с возможностью перемещения к его началу или концу;
* добавление уникального имени нового пользователя к списку с пустым паролем (строкой нулевой длины);
* блокирование возможности работы пользователя с заданным именем;
* завершение работы с программой.

В режиме обычного пользователя программа должна поддерживать только функции смены пароля пользователя (при правильном вводе старого пароля) и завершения работы, а все остальные функции должны быть заблокированы.

После своего запуска программа должна запрашивать у пользователя в специальном окне входа ввод его имени и пароля. При вводе пароля его символы всегда должны на экране заменяться символом ‘\*’. При отсутствии введенного в окне входа имени пользователя в списке зарегистрированных администратором пользователей программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода имени или завершения работы с программой. При неправильном вводе пароля программа должна выдавать соответствующее сообщение и предоставлять пользователю возможность повторного ввода. При трехкратном вводе неверного пароля работа программы должна завершаться.

Информация о зарегистрированных пользователях, их паролях, отсутствии блокировки их работы с программой должна сохраняться в специальном файле. При первом запуске программы этот файл должен создаваться автоматически и содержать информацию только об администраторе, имеющем пустой пароль.

Интерфейс с программой должен быть организован на основе меню, обязательной частью которого должно являться подменю «Справка» с командой «О программе». При выборе этой команды должна выдаваться информация об авторе программы и выданном индивидуальном задании. Интерфейс пользователя программы может также включать панель управления с дублирующими команды меню графическими кнопками и строку состояния. В программе должны использоваться диалоговые формы, позволяющие пользователю (администратору) вводить необходимую информацию.

**Задание П/Г-1**

**Часть 1: Определяемый пользователем пароль должен соответствовать определенный требованиям сложности**:

* Длина не меньше минимальной длины, устанавливаемой администратором и сохраняемой в учетной записи пользователя (индивидуально для каждого пользователя).
* Наличие строчных и прописных букв.
* Наличие цифр и знаков препинания.
* Отсутствие повторяющихся символов.

При вводе нового пароля должна выдаваться информации о выполнении (или невыполнении) каждого из указанных выше требований.

**Часть 2: Идентификация пользователей также может осуществляться по сертификату, записанному на USB-носителе** (при установке соответствующего параметра учетной записи пользователя). В данном случае программа должна выявлять факт наличия сертификата на подключенном USB-носителе, считывать его и выполнять необходимые операции по проверке прав доступа и входу пользователя в систему.

При использовании USB-носителя основные параметры учетной записи пользователя хранятся на носителе, в то же время программ должна проверять корректность (легальность) сертификата.

В настройках программы должна задаваться и храниться информация об имени диска, предназначенного для носителей с сертификатами.

**Краткое описание сертификата открытого ключа**

Сертификат открытого ключа - это структура данных, обеспечивающая ассоциирование открытого ключа и его владельца. Надежность ассоциации, подлинность сертификата подтверждаются подписью удостоверяющего центра (УЦ).

Сертификаты имеют конечный срок годности. Поддерживать актуальность информации об их статусе помогают списки отзыва, подписываемые удостоверяющими центрами и содержащими перечни сертификатов, переставших быть годными. Последнее может случиться как в результате естественного окончания срока, так и досрочно, например, из-за компрометации секретного ключа владельца.

Формат сертификата в простейшем случае выглядит так:

CA <<A>> = CA {V, SN, AI, CA, A, Ap, TA}

Здесь:

* A - имя владельца сертификата;
* CA - имя удостоверяющего центра;
* CA <<A>> - сертификат, выданный A центром CA;
* CA {I} - данные I, снабженные подписью CA;
* V - версия сертификата;
* SN - порядковый номер сертификата;
* AI - идентификатор алгоритма, использованного при подписании сертификата;
* Ap - информация об открытом ключе A;
* TA - даты начала и конца срока годности сертификата.

Формат сертификата может быть существенно сложнее. С помощью механизма расширений его можно приспособить для нужд различных приложений и сообществ пользователей.

Для шифрования и цифровой подписи применяют разные ключи; следовательно, у одного субъекта может быть несколько пар ключей и, соответственно, несколько сертификатов. Чтобы выбрать среди них нужный, необходимо иметь возможность выяснить назначение представленного в сертификате открытого ключа. Аналогично, может потребоваться знание срока годности секретного ключа, посредством которого формируют ЭЦП, поскольку этот срок обычно меньше, чем у открытого ключа, проверяющего подпись.

**Задание П/Г-2**

**Часть 1: Определяемый пользователем пароль должен соответствовать определенный требованиям сложности:**

* Длина не меньше минимальной длины, устанавливаемой администратором (для всех пользователей).
* Наличие латинских букв, символов кириллицы и знаков арифметических операций.
* Отсутствие подряд расположенных одинаковых символов.
* Несовпадение с именем пользователя, записанным в обратном порядке.

При вводе нового пароля должна выдаваться информации о выполнении (или невыполнении) каждого из указанных выше требований.

**Часть 2: В программу должен быть встроен механизм защиты от несанкционированного использования и копирования.**Программа должна выдавать сообщение в случае обнаружения несанкционированного использования и копирования и завершаться. В сообщении должно указываться, какие требования (контролируемые параметры были нарушены).

Во время установки программа собирает информацию о компьютере, на котором устанавливается программа, кодирует/шифрует эту информацию (в дальнейшем – Сигнатуру компьютера) и записывает ее в реестр в раздел HKEY\_CURRENT\_USER \Software\Фамилия\_студента как значение параметра Signature или файл настроек (в файле настроек должна быть предусмотрена защита от несанкционированных изменений).  
Периодически программа генерирует и проверяет сигнатуру.

Собираемая о компьютере информация включает в себя:

* имя пользователя системы,
* имя компьютера,
* путь к папке с ОС Windows,
* ширина и высота экрана,
* данные об объеме ОЗУ, объеме, метке типе файловой системы HDD.

**Проверка реализации функций (20 пунктов проверки)**

Общие функции:

1. Наличие двух режимов работы (администратор).
2. Наличие двух режимов работы (пользователь).
3. Логин администратора фиксирован (ADMIN).
4. ADMIN - Смена пароля (при правильном вводе старого пароля).
5. ADMIN - Просмотр списка имен зарегистрированных пользователей и установленных для них параметров.
6. ADMIN - Добавление уникального имени нового пользователя к списку с пустым паролем.
7. ADMIN - Блокирование возможности работы пользователя с заданным именем.
8. USER - Только функции смены пароля пользователя.
9. При вводе пароля его символы всегда должны на экране заменяться символом ‘\*’.
10. Повторный ввод имени пользователя или завершение работы с программой (при неправильном вводе).
11. При трехкратном вводе неверного пароля работа программы должна завершаться.
12. Информация о зарегистрированных пользователях должна сохраняться в специальном файле (создается при первом запуске с пользователем ADMIN).
13. Подменю «Справка» с командой «О программе» (информация об авторе программы и выданном индивидуальном задании).

ПГ1:

1. Требования сложности пароля - Длина не меньше минимальной длины, устанавливаемой администратором и сохраняемой в учетной записи пользователя (индивидуально для каждого пользователя).
2. Требования сложности пароля - Наличие строчных и прописных букв.
3. Требования сложности пароля - Наличие цифр и знаков препинания.
4. Требования сложности пароля - Отсутствие повторяющихся символов.
5. Определение наличия сертификата на USB-носителе.
6. Сертификат - параметры учетной записи пользователя хранятся на носителе (отсутствуют в локальном файле пользователей).
7. В настройках программы должна задаваться и храниться информация об имени диска, предназначенного для носителей с сертификатами.

ПГ2:

1. Требования сложности пароля - Длина не меньше минимальной длины, устанавливаемой администратором (для всех пользователей).
2. Требования сложности пароля - Наличие латинских букв, символов кириллицы и знаков арифметических операций.
3. Требования сложности пароля - Отсутствие подряд расположенных одинаковых символов.
4. Требования сложности пароля - Несовпадение с именем пользователя, записанным в обратном порядке.
5. Сообщение в случае обнаружения несанкционированного использования и копирования (с указанием нарушенных параметров).
6. Сигнатура компьютера записана.

Для расчета сигнатуры используются 5 параметров (имя пользователя системы, имя компьютера, путь к папке с ОС Windows, ширина и высота экрана, данные об объеме ОЗУ, объеме, метке типе файловой системы HDD).

## Особенности реализации лабораторной работы 1

В общем случае программа должна обеспечивать работу в двух режимах: администратора (пользователя с фиксированным именем ADMIN) и обычного пользователя. Админ определяет параметры работы с программой.

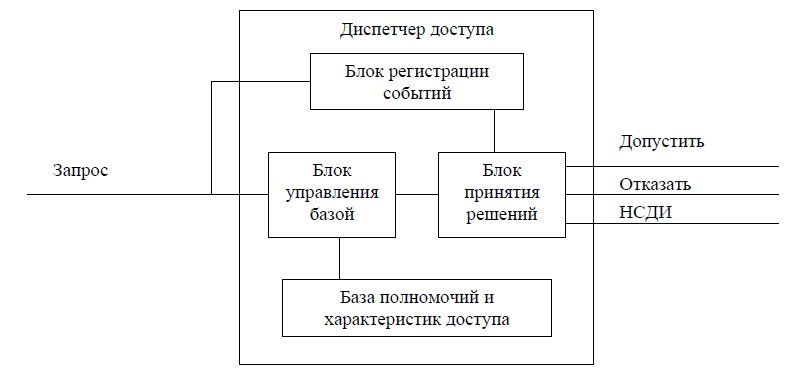
Программа должна быть реализована с учетом требований к реализации систем разграничения доступа (СРД) к информации.

Система разграничения доступа к информации должна содержать четыре функциональных блока:

* блок идентификации и аутентификации субъектов доступа;
* диспетчер доступа;
* блок криптографического преобразования информации при ее хранении и передаче;
* блок очистки памяти.

Идентификация и аутентификация субъектов осуществляется в момент их доступа к устройствам, в том числе и дистанционного доступа.

Диспетчер доступа реализуется в виде аппаратно-программных механизмов (рис.) и обеспечивает необходимую дисциплину разграничения доступа субъектов к объектам доступа (в том числе и к аппаратным блокам, узлам, устройствам). Диспетчер доступа разграничивает доступ к внутренним ресурсам КС субъектов, уже получивших доступ к этим системам.



Запрос на доступ i-го субъекта и j-му объекту поступает в блок управления базой полномочий и характеристик доступа и в блок регистрации событий. Полномочия субъекта и характеристики объекта доступа анализируются в блоке принятия решения, который выдает сигнал разрешения выполнения запроса, либо сигнал отказа в допуске. Если число попыток субъекта допуска получить доступ к запрещенным для него объектам превысит определенную границу (обычно 3 раза), то блок принятия решения на основании данных блока регистрации выдает сигнал «НСДИ» (несанкционированный доступ к информации) администратору системы безопасности. Администратор может блокировать работу субъекта, нарушающего правила доступа в системе, и выяснить причину нарушений.

Кроме преднамеренных попыток НСДИ диспетчер фиксирует нарушения правил разграничения, явившихся следствием отказов, сбоев аппаратных и программных средств, а также вызванных ошибками персонала и пользователей.

Следует отметить, что в распределенных КС криптографическое закрытие информации является надежным единственным способом защиты от НСДИ.

В СРД должна быть реализована функция очистки оперативной памяти и рабочих областей на внешних запоминающих устройствах после завершения выполнения программы, обрабатывающей конфиденциальные данные. Причем очистка должна производиться путем записи в освободившиеся участки памяти определенной последовательности двоичных кодов, а не удалением только учетной информации о файлах из таблиц ОС, как это делается при стандартном удалении средствами ОС.

## Лабораторная работа 2. Защита программного обеспечения от изменения и копирования

**Цель работы**

Изучение методов защиты ПО от изменения и копирования.

**Задание**

* Изучить возможности защиты программ (лицензирования) с использованием предложенного программного обеспечения (Obsidium, WinLicense). Демоверсию скачать на сайте разработчика. Защитить каждой из программ по одному приложению (от копирования, триал-версия, лицензирование).
* Реализовать защиту pdf файла с использованием встроенных javascript (содержимое документа отображается при вводе пароля в форме pdf документа, сам документ защищен паролем от копирования содержимого и печати). При реализации документа (для размещения полей формы и javascript) можно использовать Scribus.
* Реализовать **собственную** DRM систему защиты файлов (txt, doc/x, pdf) с использованием собственного просмотрщика и модуля управления лицензиями (при реализации сервера управления лицензиями - задание можно выполнять в группе). Лицензирование по ключам и с привязкой к параметрам профиля пользователя или компьютера (операционной системы).

Результаты работы можно использовать при выполнении ЛР-3 «Разработка и программная реализация криптографических алгоритмов».

## Лабораторная работа 3. Разработка и программная реализация криптографических алгоритмов

**Цель работы**

Изучение методов криптографической защиты данных.

**Задание**

* Реализовать программу осуществляющую шифрование (и дешифрование) файлов.

Способ/алгоритм шифрования выбирается самостоятельно. Рекомендуется, чтобы действия программы определялись через параметры командной строки.

Программа должна содержать справку, которая выдается при ее запуске без параметров.

В случае, если программе в качестве параметра не передан ключ (пароль), программа должна осуществлять его генерирование (пароль должен отвечать требованиям сложности, аналогично требованиям ЛР №1 по подгруппам).

## Лабораторная работа 4. Изучение способов формирования электронной цифровой подписи (ЭЦП) на основе КриптоПро CSP 3.9 R2 / КриптоПро CSP 4.0 - для Windows 10

**Цель работы**

Изучение принципов работы УЦ, исследование процесса установки УЦ КриптоПро на ОС MS Windows 10.

**Задание**

* Установить и настроить УЦ КриптоПро.
* Выпустить ЭЦП пользователя. В качестве пользователя выступает студент, выполняющий работу.
* Дистрибутив демоверсии ПО КриптоПро CSP 3.9 R2 / КриптоПро CSP 4.0 скачать с сайта разработчика.
* Следовать инструкциям по установке КриптоПро CSP 3.9 R2 / КриптоПро CSP 4.0

К лабораторной работе прилагаются инструкция по установке.

**Лабораторная работа 5. Изучение способов формирования электронной цифровой подписи (ЭЦП) на основе ViPNet CSP 4.2 - для Windows 10**

**Цель работы**

Изучение принципов работы УЦ, исследование процесса установки ViPNet CSP 4.2 на ОС MS Windows 10.

**Задание**

* Установить и настроить ViPNet CSP 4.2 (<https://infotecs.ru/downloads/beta-versii/vipnet-csp.html?arrFilter_93=1824101684&set_filter=Y>)
* Выпустить ЭЦП пользователя. В качестве пользователя выступает студент, выполняющий работу.
* Дистрибутив демоверсии ПО ViPNet CSP 4.2 скачать с сайта разработчика.
* Следовать инструкциям по установке ViPNet CSP 4.2

Инструкция по установке взять с сайта разработчика https://infotecs.ru/

**Лабораторная работа 6. Организация защищенного обмена информацией на основе использования программы PGP**

**Цель работы:** ознакомиться с возможностями системы PGP для защищенного хранения файлов на жестком диске.

**Задание**

* Установить приложение PGP Destop (бесплатная версия)
* С помощью PGP создайте файл и отправьте его на защищенное хранение. Изучите различные механизмы для шифрования и расшифровки файлов.

**Порядок выполнения работы:**

* С помощью текстового процессора Microsoft Word создайте произвольный документ и сохраните его под именем pgp-Proba.doc. Можно также сохранить под этим именем какой-либо из уже существующих файлов документов.
* Откройте этот документ в программе Microsoft Word и дайте команду Правка / Выделить все. Нажмите комбинацию клавиш CTRL+C.
* Щелкните правой кнопкой мыши на значке PGP Destop на панели индикации и выберите в контекстном меню команду Current WindowEncryptSign (Зашифровать и подписать).
* В открывшемся диалоговом окне перетащите созданный вами ключ в список Recipients (Получатели) и щелкните на кнопке ОК.
* Сохраните документ под именем pgp-Proba-clp.doc. Закройте программу Microsoft Word.
* Запустите программу Проводник и откройте папку, в которой лежит файл pgp-Proba.doc.
* Щелкните правой кнопкой мыши на значке файла и выберите в контекстном меню команду PGP Secure “pgp-Proba-doc.doc with passphrase…(защита при помощи парольной фразы). Далее следует вести парольную фразу щелкнуть на кнопу Далее.
* В окне Sing and Save (подписать и сохранить) контекстного меню Singing Key, выполняется подписка ключом. Также можно изменить локацию сохраняемого файла, в меню Save Location. Затем нажимаем Далее Готово.
* Убедитесь, что в папке появился файл pgp-Proba.doc.pgp.
* Теперь расшифруем созданные файлы. Запустите программу Microsoft Word и откройте файл pgp-Proba-clp.doc.
* Щелкните правой кнопкой мыши на значке PGP Desktop на панели индикации и выберите в контекстном меню команду Current WindowDecryptVerify (Текущее окно / Расшифровать и проверить).
* В открывшемся диалоговом окне Text Viewer (Просмотр текста) щелкните на кнопке Copy to Clipboard (Скопировать в буфер обмена).
* Вставьте текст в окно программы Microsoft Word и сохраните полученный файл.
* Через программу Проводник разыщите файл pgp-Proba.doc.pgp. Дважды щелкните на его значке.
* Введите парольную фразу и щелкните на кнопке ОК.
* Затем, щелкнув на файл правой кнопкой и выбрав команду Extract (извлечь), следует указать адрес (место положение) извлекаемого файла.

В процессе работы студент учится отправлять файлы на защищенное хранение, шифруя их при помощи программы PGP. Для текстовых данных эту операцию можно применять непосредственно в текущем окне редактора или к данным, находящимся в буфере обмена. Для произвольных файлов выполнять шифрование можно через контекстное меню.

## Лабораторная работа 7. Организация защищенного канала с помощью VPN

**Цель работы**

Изучение механизмов построения защищенных с VPN сетей.

**Задание**

* Изучить возможности организации VPN при использовании СЗИ VipNet, возможности использования IPSec для шифрования и экранирования трафика.
* Воспроизвести последовательность настройки указанных средств, приведенную в файле VPN.pdf (возможны некоторые несоответствия).
* Проверить работоспособность системы путем перехвата и анализа трафика.

К лабораторной работе прилагаются видеоматериалы.

## Лабораторная работа 8. Программная реализация защиты программ с помощью электронных ключей типа «HASP HL Pro»

**Цель работы**

Изучение принципов защиты информации с помощью электронных ключей типа «HASP HL Pro»

**Задание**

* Установить ПО в комплекте с ключом типа «HASP HL Pro»
* Защитить приложение с помощью «HASP HL Pro»
* Проверить работоспособность системы
* Проверить работоспособность для защищаемого приложения в режиме клиент-сервер

**Список литературы:**

а) основная литература:

* Программно-аппаратные средства защиты информационных систем: учебное пособие : [16+] / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2017. – 194 с. ISBN 978-5-8265-1737-6.
* Технологии обеспечения безопасности информационных систем : учебное пособие: [16+] / А. Л. Марухленко, Л. О. Марухленко, М. А. Ефремов и др. – Москва ; Берлин : Директ-Медиа, 2021. – 210 с ISBN 978-5-4499-1671-6. – DOI 10.23681/598988
* Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем: курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. – Томск: ТУСУР, 2016. – 396с
* Технологии защиты информации в компьютерных сетях / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 369 с.
* Долозов, Н. Л. Программные средства защиты информации: конспект лекций / Н. Л. Долозов, Т. А. Гультяева ; Новосибирский государственный технический университет. – Новосибирск : Новосибирский государственный технический университет, 2015. – 63 с. ISBN 978-5-7782-2753-8

б) дополнительная литература:

* Белоус, А. И. Основы кибербезопасности: стандарты, концепции, методы и средства обеспечения : [16+] / А. И. Белоус, В. А. Солодуха. – Москва : Техносфера, 2021. – 482 с. ISBN 978-5-94836-612-8.
* Белоус, А. И. Программные и аппаратные трояны — способы внедрения и методы противодействия: первая техническая энциклопедия : в 2 книгах / А. И. Белоус, В. А. Солодуха, С. В. Шведов. – Москва: Техносфера, 2019. – Книга 1. – 1318 с. ISBN 978-5-94836-524-4
* Мэйволд, Э. Безопасность сетей : учебное пособие : [16+] / Э. Мэйволд. – 2-е изд., испр. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 572 с.
* Басыня, Е. А. Системное администрирование и информационная безопасность: учебное пособие: [16+] / Е. А. Басыня. – Новосибирск: Новосибирский государственный технический университет, 2018. 79с. ISBN 978-5-7782-3484-0. – Текст : электронный.

в) программное обеспечение и Интернет-ресурсы:

* Нормативные правовые акты, организационно-распорядительные документы, по технической защите информации ФСТЭК России. URL: <http://fstec.ru/>
* Курсы НОУ «ИНТУИТ» по разделам дисциплины. URL: <http://www.intuit.ru/studies/courses>
* Сайт «Группа СТ» г. Санкт-Петербург [Электронный ресурс] // URL: <http://spymarket.com/>
* Сайт «Группа компаний «Маском»» г.Москва [Электронный ресурс] // URL: <http://www.mascom.ru/> (дата обращения: 13.06.2018).
* Сайт ЗАО НПЦ Фирма "НЕЛК" г. Москва [Электронный ресурс] // URL: <https://www.nelk.ru/>
* Сайт «НПО Защита информации» г. Москва [Электронный ресурс] // URL: <http://www.sinf.ru/>
* Документация на ПО, представленная на сайтах производителей ПО.