Учреждения образования

«Белорусский государственный технологический университет»

**Кафедра Информационных систем и технологий**

**Отчеты по практическим работам**

По дисциплине: «Основы защиты информации»

Выполнил:

Студент 2 курса 3 группы ФИТ

Шкабров Данила Сергеевич

2022 г.

**Практическое занятие №1**

**Тема «Концепция национальной безопасности Республики Беларусь»**

Цель: изучить национальную концепцию национальной безопасности РБ.

Контрольные вопросы:

1. Что такое информационная безопасность?

Информационная безопасность - состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

1. Перечислить основные национальные интересы в информационной сфере?

Реализация конституционных прав граждан на получение, хранение и распространение полной, достоверной и своевременной информации;

Формирование и поступательное развитие информационного общества;

Равноправное участие Республики Беларусь в мировых информационных отношениях;

Преобразование информационной индустрии в экспортно-ориентированный сектор экономики;

Эффективное информационное обеспечение государственной политики;

Обеспечение надежности и устойчивости функционирования критически важных объектов информатизации.

1. Основные угрозы национальной безопасности, связанные с ИТ-сферой?

Внутренние:

Распространение недостоверной или умышленно искаженной информации, способной причинить ущерб национальным интересам Республики Беларусь;

Зависимость Республики Беларусь от импорта информационных технологий, средств информатизации и защиты информации, неконтролируемое их использование в системах, отказ или разрушение которых может причинить ущерб национальной безопасности;

Несоответствие качества национального контента мировому уровню;

Недостаточное развитие государственной системы регулирования процесса внедрения и использования информационных технологий;

Рост преступности с использованием информационно-коммуникационных технологий;

Недостаточная эффективность информационного обеспечения государственной политики;

Несовершенство системы обеспечения безопасности критически важных объектов информатизации.

1. Назвать основные внутренние и внешние источники угроз национальной безопасности в информационной сфере?

Внешние:

Открытость и уязвимость информационного пространства Республики Беларусь от внешнего воздействия;

Доминирование ведущих зарубежных государств в мировом информационном пространстве, монополизация ключевых сегментов информационных рынков зарубежными информационными структурами;

Информационная деятельность зарубежных государств, международных и иных организаций, отдельных лиц, наносящая ущерб национальным интересам Республики Беларусь, целенаправленное формирование информационных поводов для ее дискредитации;

Нарастание информационного противоборства между ведущими мировыми центрами силы, подготовка и ведение зарубежными государствами борьбы в информационном пространстве;

Развитие технологий манипулирования информацией;

Препятствование распространению национального контента Республики Беларусь за рубежом;

Широкое распространение в мировом информационном пространстве образцов массовой культуры, противоречащих общечеловеческим и национальным духовно-нравственным ценностям;

Попытки несанкционированного доступа извне к информационным ресурсам Республики Беларусь, приводящие к причинению ущерба ее национальным интересам.

1. Основные направления нейтрализации внутренних источников угроз и защиты от внешних угроз национальной безопасности в информационной сфере?

В информационной сфере с целью нейтрализации внутренних источников угроз национальной безопасности совершенствуются механизмы реализации прав граждан на получение, хранение, пользование и распоряжение информацией, в том числе с использованием современных информационно-коммуникационных технологий. Государство гарантирует обеспечение установленного законодательством порядка доступа к государственным информационным ресурсам, в том числе удаленного, и возможностям получения информационных услуг. Значимым этапом станет разработка и реализация стратегии всеобъемлющей информатизации, ориентированной на развитие электронной системы осуществления административных процедур, оказываемых гражданам и бизнесу государственными органами и иными организациями, и переход государственного аппарата на работу по принципу информационного взаимодействия. Ускоренными темпами будет развиваться индустрия информационных и телекоммуникационных технологий. Особое внимание будет уделяться последовательному повышению качества, объема и конкурентоспособности национального контента, который призван занимать доминирующее положение внутри страны, и его продвижению во внешнее информационное пространство.

Приоритетным направлением является совершенствование нормативной правовой базы обеспечения информационной безопасности и завершение формирования комплексной государственной системы обеспечения информационной безопасности, в том числе путем оптимизации механизмов государственного регулирования деятельности в этой сфере. При этом важное значение отводится наращиванию деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством. Активно продолжится разработка и внедрение современных методов и средств защиты информации в информационных системах, используемых в инфраструктуре, являющейся жизненно важной для страны, отказ или разрушение которой может оказать существенное отрицательное воздействие на национальную безопасность.

Вывод: в ходе практической работы я изучил национальную концепцию национальной безопасности РБ.

**Практическое занятие №2**

**Тема «Решение задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа»**

Цель: научиться решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № варианта | *E*0 | *E* | *K* | *C* |
| 15 | 26000 | 20000 | 7 | 3000 |

Решение:

Найдем, на какую величину уменьшается полезный эффект функционирования объекта:

Рассчитаем относительную эффективность:

Найдем снижение эффективности функционирования объекта:

В итоге формулы выше принимают следующий вид:

Если эффективность функционирования объекта имеет стоимостное выражение (доход, прибыль и т.д.), то UΣ (суммарный ущерб) непосредственно изменяет эффективность:

Вывод: в ходе практической работы я научился решать задачи разработки средств защиты для обеспечения максимальной эффективности объекта в условиях несанкционированного доступа.

**Практическое занятие №3**

**Тема «Разработка политики информационной безопасности бизнес-компании»**

**Введение**

Политика безопасности – это комплекс предупредительных мер по обеспечению информационной безопасности организации. Политика безопасности включает правила, процедуры и руководящие принципы в области безопасности, которыми руководствуется организация в своей деятельности. Кроме этого, политика безопасности включает в себя требования в адрес субъектов информационных отношений, при этом в политике безопасности излагается политика ролей субъектов информационных отношений.

Прежде всего политика необходима для того, чтобы донести до бизнеса цели и задачи информационной безопасности компании. Бизнес должен понимать, что агент безопасности – это не только инструмент для расследования фактов утечек данных, но и помощник в минимизации рисков компании, а, следовательно, ­­­­­­­­– в повышении прибыльности компании.

**Описание структуры компании**

В настоящее время под организационной структурой понимается упорядоченная совокупность устойчиво взаимосвязанных элементов, обеспечивающих функционирование и развитие организации как единого целого. Структура управления определяется также как форма разделения и кооперации управленческой деятельности. Можно сказать, что структура управления есть не что иное, как оптимальное распределение работы, прав и ответственности, порядка и форм взаимодействия между членами коллектива организации.

Опишем структуру Интернет-магазина «Вектор (техника)»:

1. Директор
2. Главный бухгалтер
   1. Бухгалтерия
3. Менеджер
4. Продавцы-консультанты

**Оценка рисков**

Идентифицировать и оценить активы, разработать модель нарушителя и модель угроз, идентифицировать уязвимости – все это стандартные шаги, описание которых должно присутствовать в любой методике анализа рисков. Все перечисленные шаги могут выполняться с различным уровнем качества и детализации. Очень важно понять, что и как можно сделать с огромным количеством накопленной информации и формализованными моделями. На наш взгляд, этот вопрос наиболее важен, и ответ должна давать используемая методика анализа рисков.

Полученные результаты необходимо оценить, агрегировать, классифицировать и отобразить. Так как ущерб определяется на этапе идентификации и оценки активов, необходимо оценить вероятность событий риска. Как и в случае с оценкой активов, оценку вероятности можно получить на основании статистики по инцидентам, причины которых совпадают с рассматриваемыми угрозами ИБ, либо методом прогнозирования – на основании взвешивания факторов, соответствующих разработанной модели угроз.

**Сущность любого подхода к управлению рисками заключается в анализе факторов риска и принятии адекватных решений по обработке рисков. Факторы риска – это те основные параметры, которыми мы оперируем при оценке рисков. Таких параметров всего семь:**

* **актив;**
* **ущерб;**
* **угроза;**
* **уязвимость;**
* **механизм контроля;**
* **размер среднегодовых потерь;**
* **возврат инвестиций.**

На второй фазе, которая определяется стандартами как оценивание рисков, необходимо ответить на вопрос: Какой уровень риска является приемлимым для организации и, исходя из этого, какие риски превышают этот уровень.

Такиим образом, по результатам оценки рисков, мы получаем описание рисков, превышающих допустимый уровень и оценку величины этих рисков, которая определяется размером среднегодовых потерь. Далее необходимо принять решение по обработке рисков, ответить на следующие вопросы:

* Какой вариант обработки рисков выбираем?
* Если принимается решение о минимизации риска, то какие механизмы контроля необходимы?
* Насколько эффективны эти механизмы контроля и какой возврат инвестиций они обеспечат?

На выходе данного процесса появляется план обработки рисков, определяющий способы обработки рисков, стоимость контрмер, а так же сроки и ответственных за реализацию контрмер.

Подводя итоги вышесказанного, обобщим их. Как уже было сказано, благодаря специфике работы, атаки являются довольно редкими, так как даже при условии успешности, прибыль довольно мала. Однако вероятность угрозы все равно присутствует и руководству компании необходимо осознавать и представлять возможные угрозы, чтобы иметь возможность подготовиться к ним и предотвратить их полностью, либо минимизировать возможный ущерб.

В связи с этим, наиболее возможными видами атаки на торговую сеть являются следующие:

* получение несанкционированного доступа к веб-сайту. Данный тип атаки наименее опасен, поскольку у сайта так же нету связи с финансовой системой сети. Однако злоумышленники могут испортить информацию на веб-сайте и благодаря этому извлечь какую-нибудь выгоду, либо осуществить «взлом» просто ради интереса;
* взлом банковского счета магазина. В настоящее время у любой компании имеется свой счет, на котором находятся деньги фирмы. Естественно, данная угроза наименее зависима от сети, так как атака осуществляется на банк. Тем не менее, компания должна предусмотреть данный случай и минимизировать его возможность;
* недобросовестная конкуренция. Данная угроза так же присутствует всегда у любой компании, независимо от ее размера, поэтому ей необходимо уделить внимание при разработке политики информационной безопасности;

Ответственными за реализацию контрмер являются, безусловно, сотрудники системы безопасности компании, наравне с сотрудниками IT-отдела, которые отвечают за информационную безопасность.

**Разработка мер защиты**

Построение надежной защиты включает оценку циркулирующей в компьютерной системе информации с целью уточнения степени ее конфиденциальности, анализа потенциальных угроз ее безопасности и установление необходимого режима ее защиты.

Эффективность защиты информации в автоматизированных системах достигается применением средств защиты информации (СЗИ). Под средством защиты информации понимается техническое, программное средство или материал, предназначенные или используемые для защиты информации. В настоящее время на рынке представлено большое разнообразие средств защиты информации, которые условно можно разделить на несколько групп:

* средства, обеспечивающие разграничение доступа к информации в автоматизированных системах;
* средства, обеспечивающие защиту информации при передаче ее по каналам связи;
* средства, обеспечивающие защиту от утечки информации по различным физическим полям, возникающим при работе технических средств автоматизированных систем;
* средства, обеспечивающие защиту от воздействия программ-вирусов;
* материалы, обеспечивающие безопасность хранения, транспортировки носителей информации и защиту их от копирования.

Наибольшая эффективность защиты информации достигается при комплексном использовании средств анализа защищенности и средств обнаружения опасных информационных воздействий (атак) в сетях. Средства обнаружения атак в сетях предназначены для осуществления контроля всего сетевого трафика, который проходит через защищаемый сегмент сети, и оперативного реагирование в случаях нападения на узлы корпоративной сети. Большинство средств данной группы при обнаружении атаки в сети оповещают администратора системы, регистрируют факт нападения в журнале системы и завершают соединение с атакующим узлом. Дополнительно, отдельные средства обнаружения атак позволяют автоматически реконфигурировать межсетевые экраны и маршрутизаторы в случае нападения на узлы корпоративной сети.

Обобщая все вышесказанное и учитывая возможные виды угрозы/атаки на торговую сеть, можем выделить следующие рекомендации, либо советы, следуя которым возможно снизить риски опасного воздействия и их последствий:

* охрана Интернет-магазина (сервера);
* четкая и строгая иерархия должностей и полномочий в магазине. Каждый должен заниматься строго своим заданием;
* обязательная экстренная связь каждого сотрудника с милицией и пожарной службой (наличие кнопок экстренного вызова) и четкий инструктаж персонала на случай чрезвычайного происшествия;
* строгий подбор сотрудников с привлечением;
* защита важной корпоративной почты;
* использование новейших средств защиты (антивирусные продукты, файерволы) персональных компьютеров сотрудников и обязательное использование лишь лицензионных продуктов;
* разграничение доступа к финансовым отделам;
* проведение регулярных бесед и инструктажей с сотрудниками;

Так же, эффективной мерой по защите является проведение тестовых экспериментов по атаке на фирму: наем специализированных людей, которые проведут атаку на сетевые ресурсы компании и выявят пробелы в защите. Данная операция безусловно является дорогостоящей, однако впоследствии, это сэкономит средства компании.

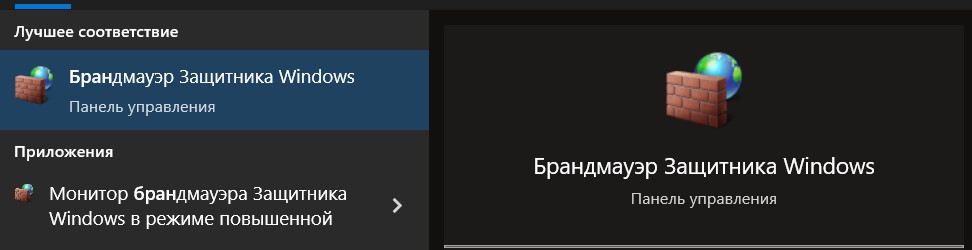
**Выводы**

Приведенные выше меры по защите информации являются лишь примерными. В реальности, следует провести комплексную оценку с привлечением специализированных людей, которые являются экспертами в вопросах обеспечения ИБ и проведением специальных тестов и экспериментов.

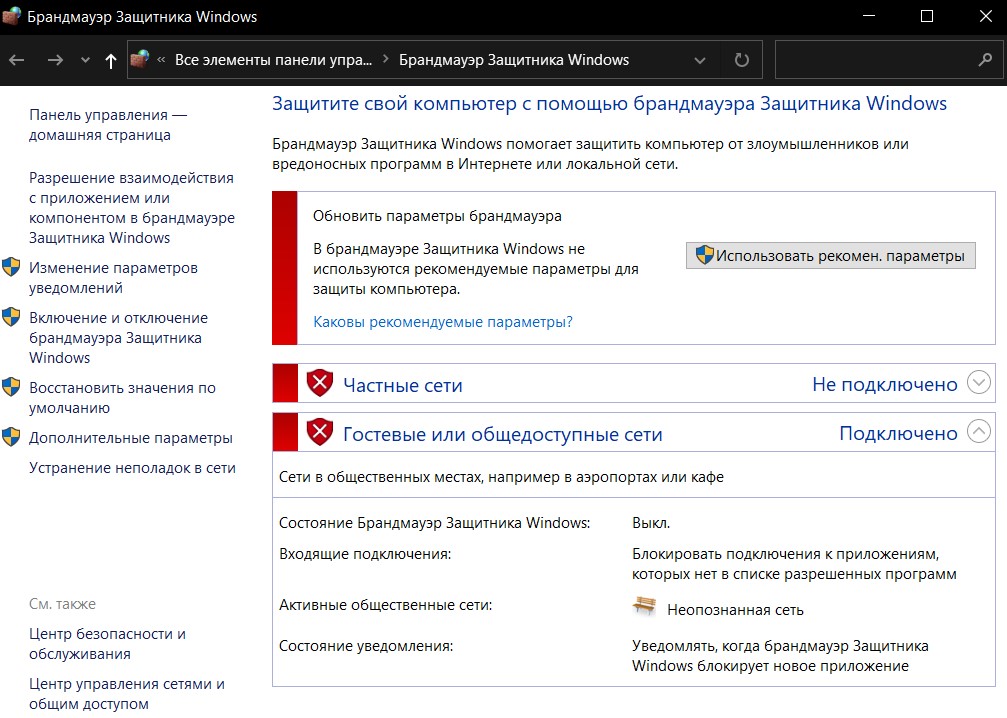
**Практическое занятие №4**

**Тема «Настройка Брандмауэра Windows»**

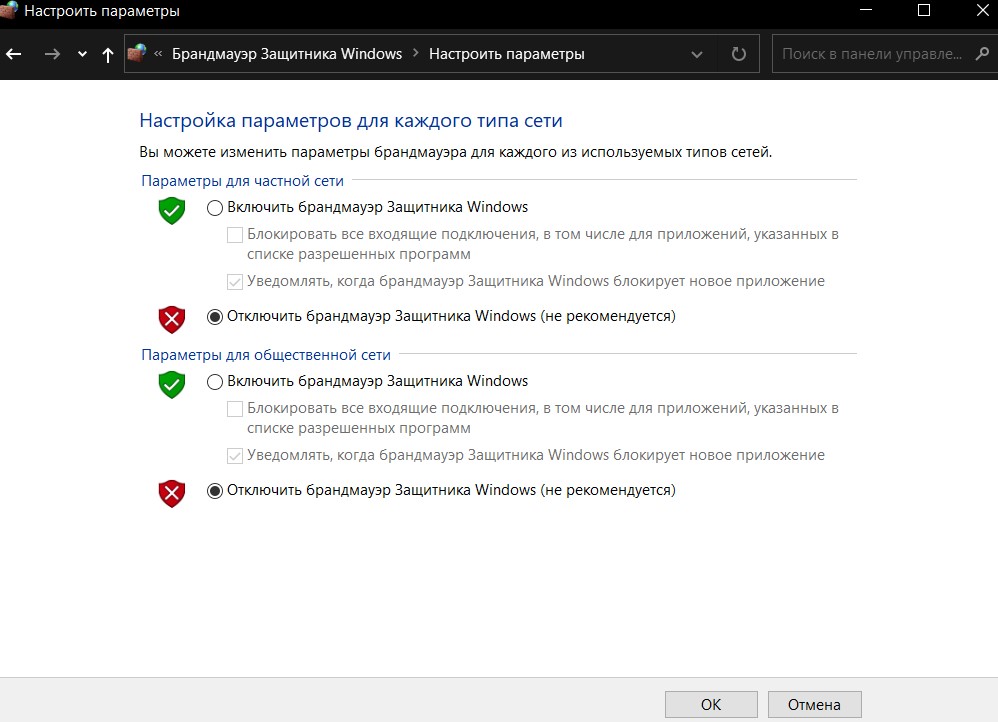
Цель: Овладение навыками настройки и использования Брандмауэра Windows.



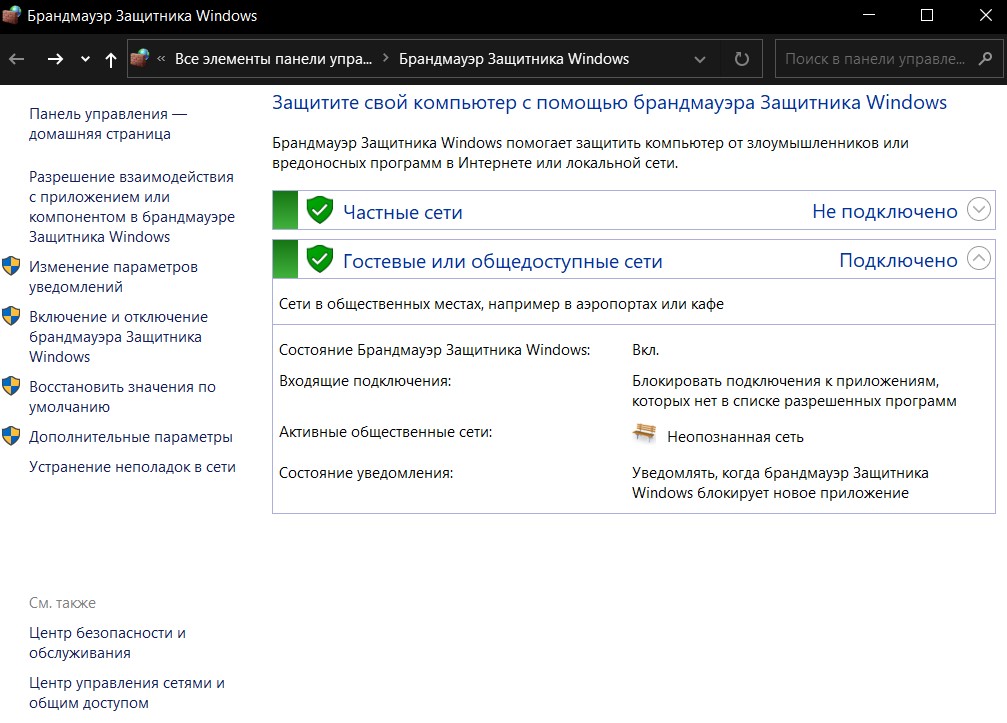
Поиск брандмауэра



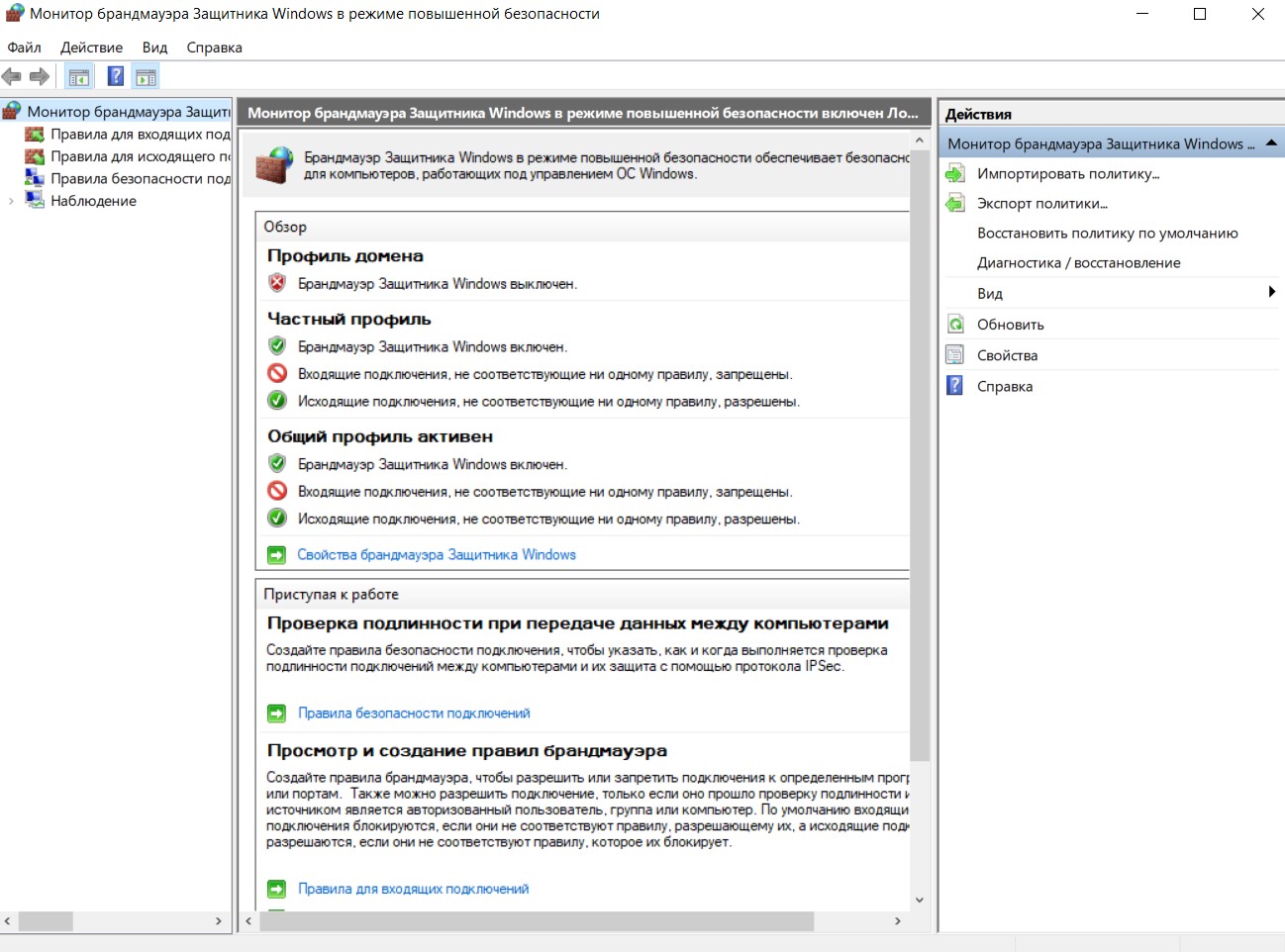
Общая информация (Выключен)



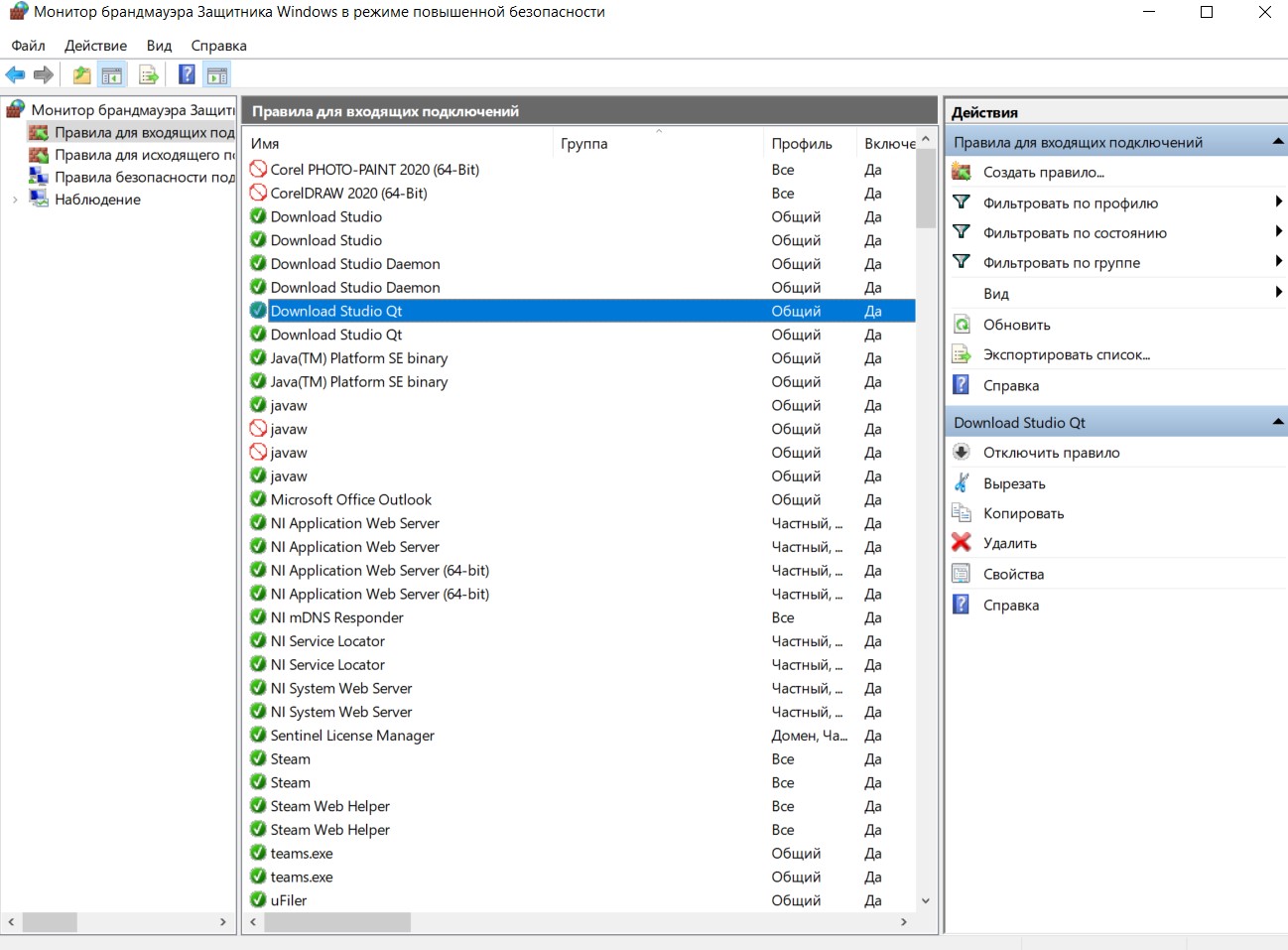
Включение и выключение брандмауэра



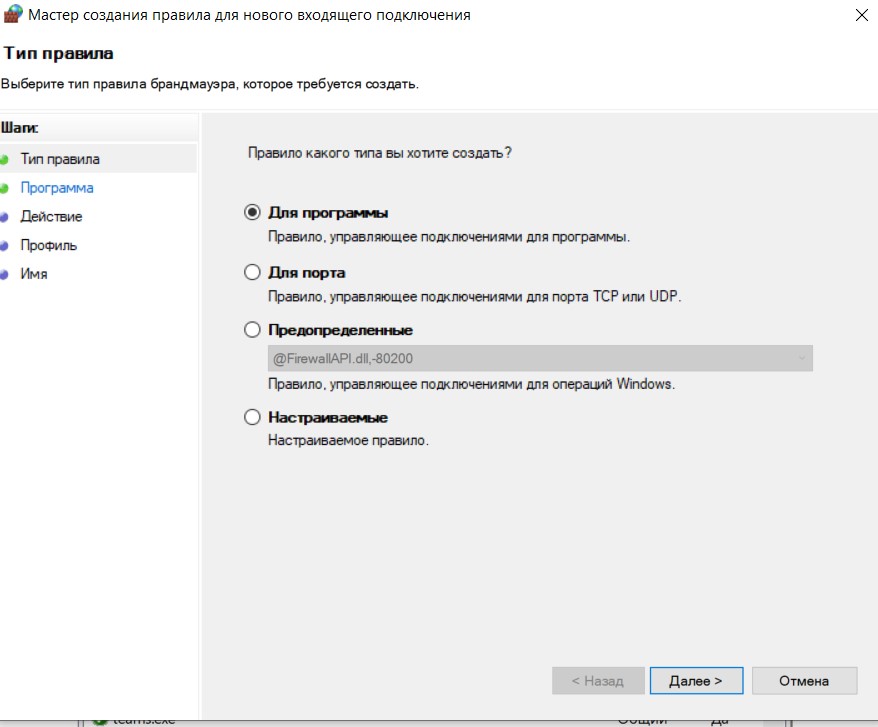
Общая информация (Включен)

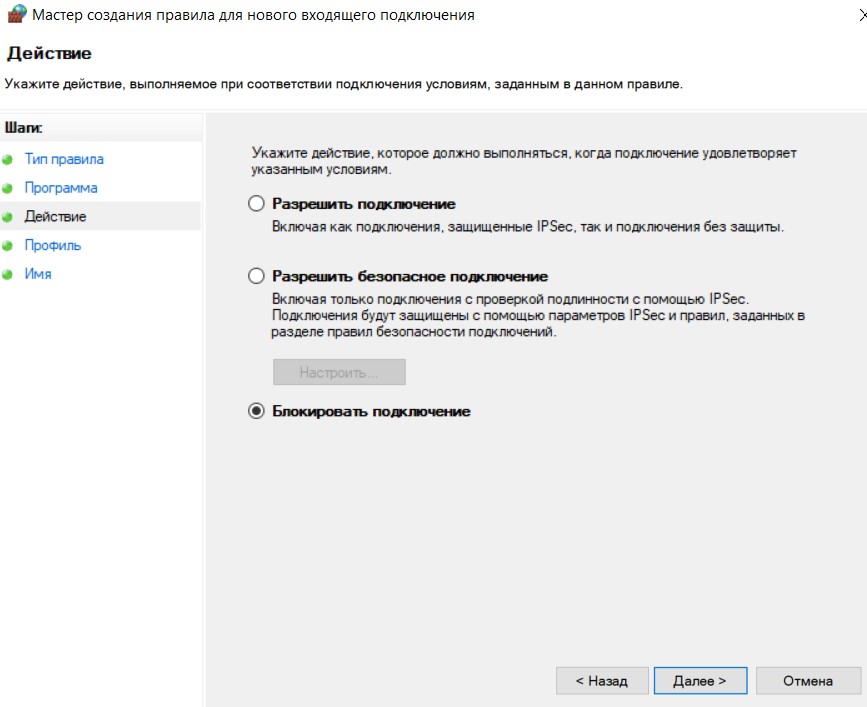


Монитор брандмауэра

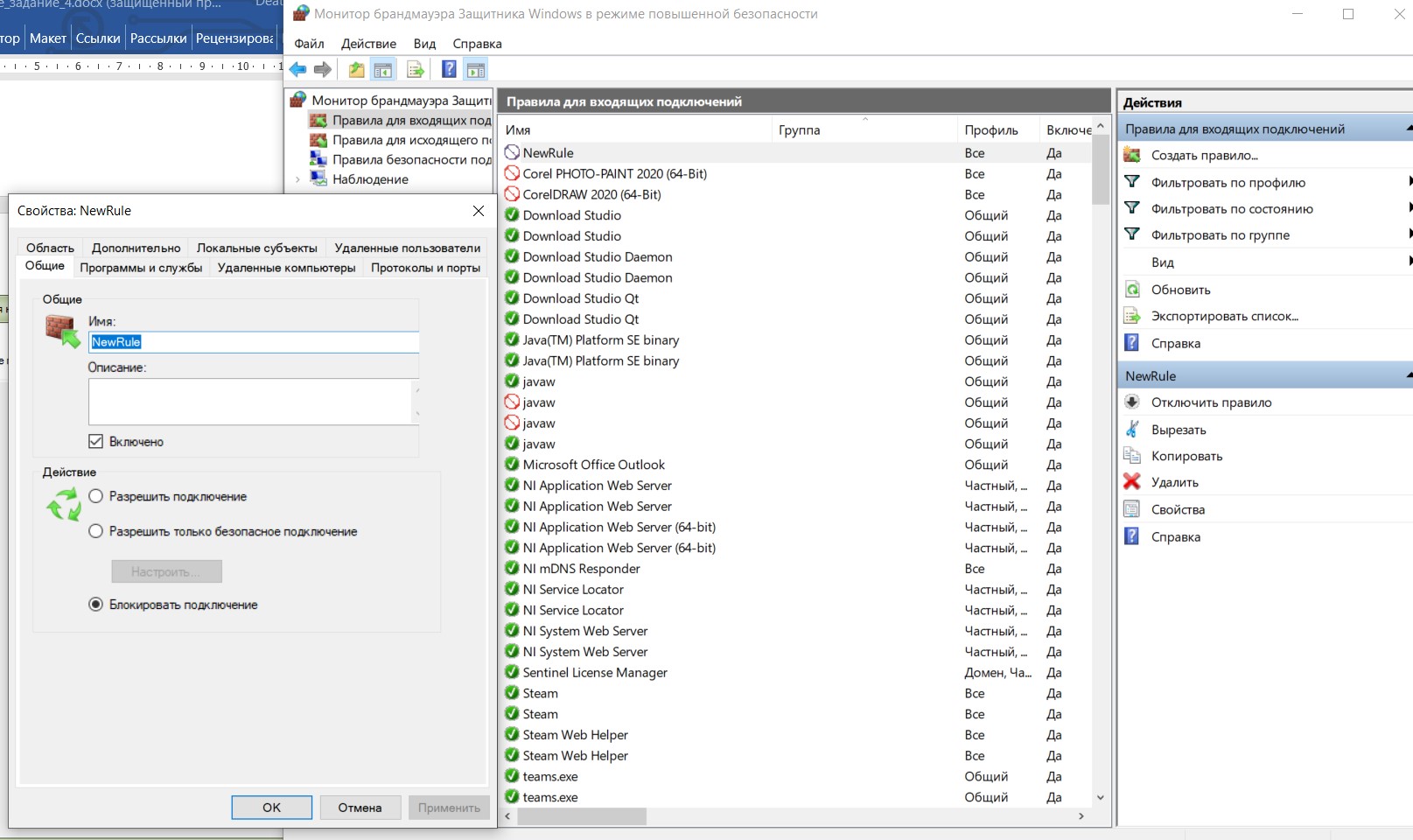


Правило для входящих

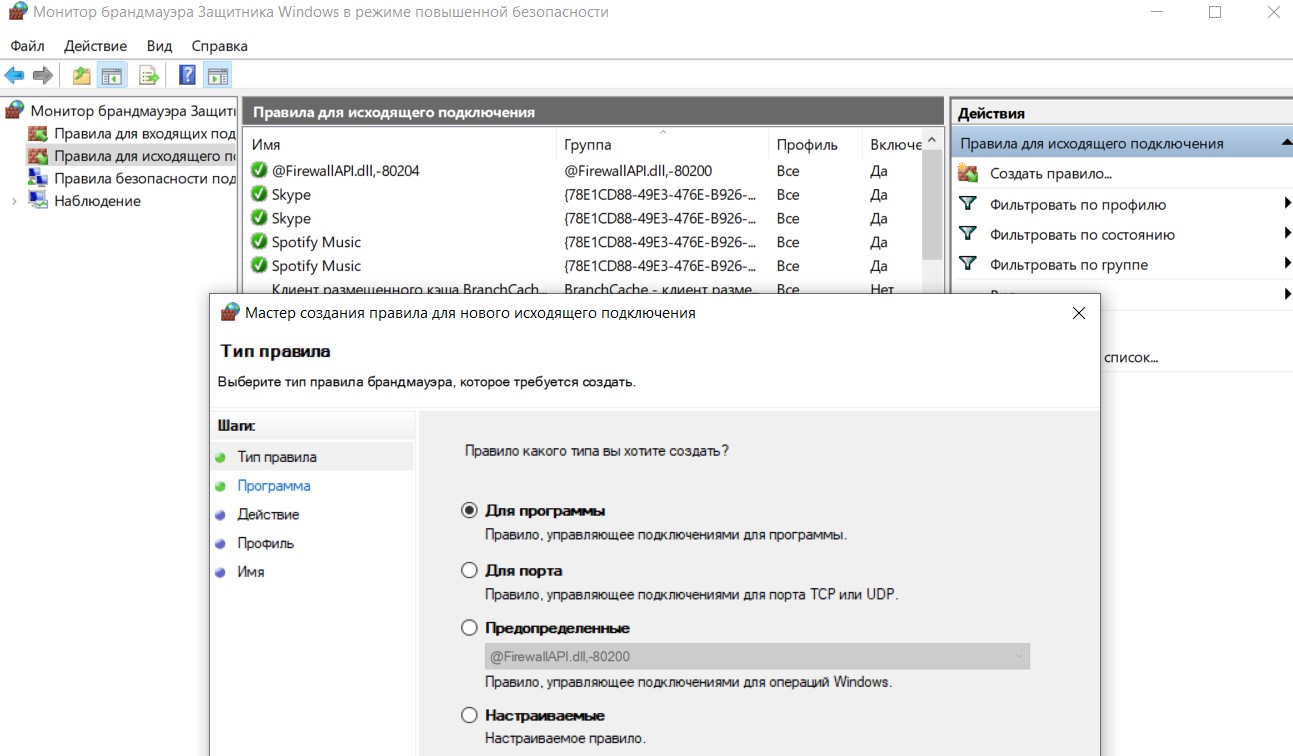


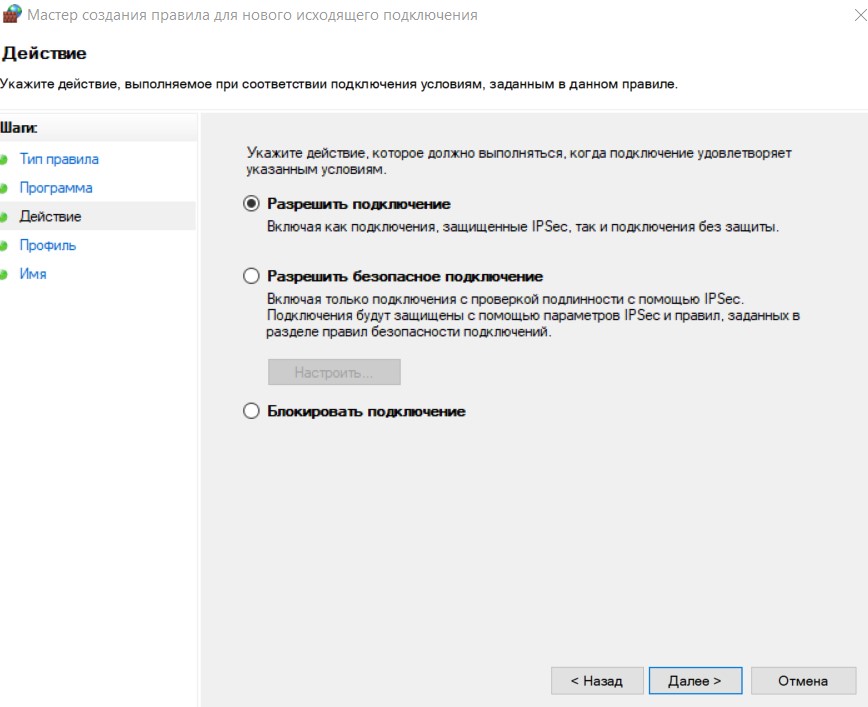


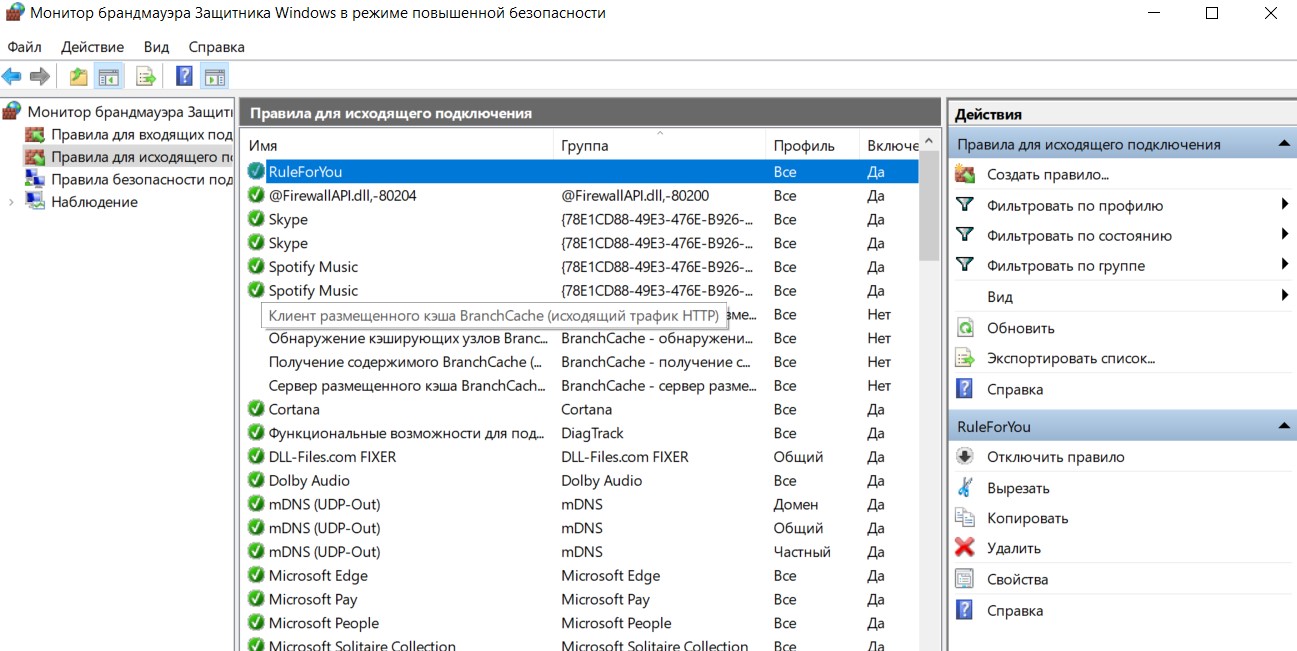
Создание правила (Блокировка его)



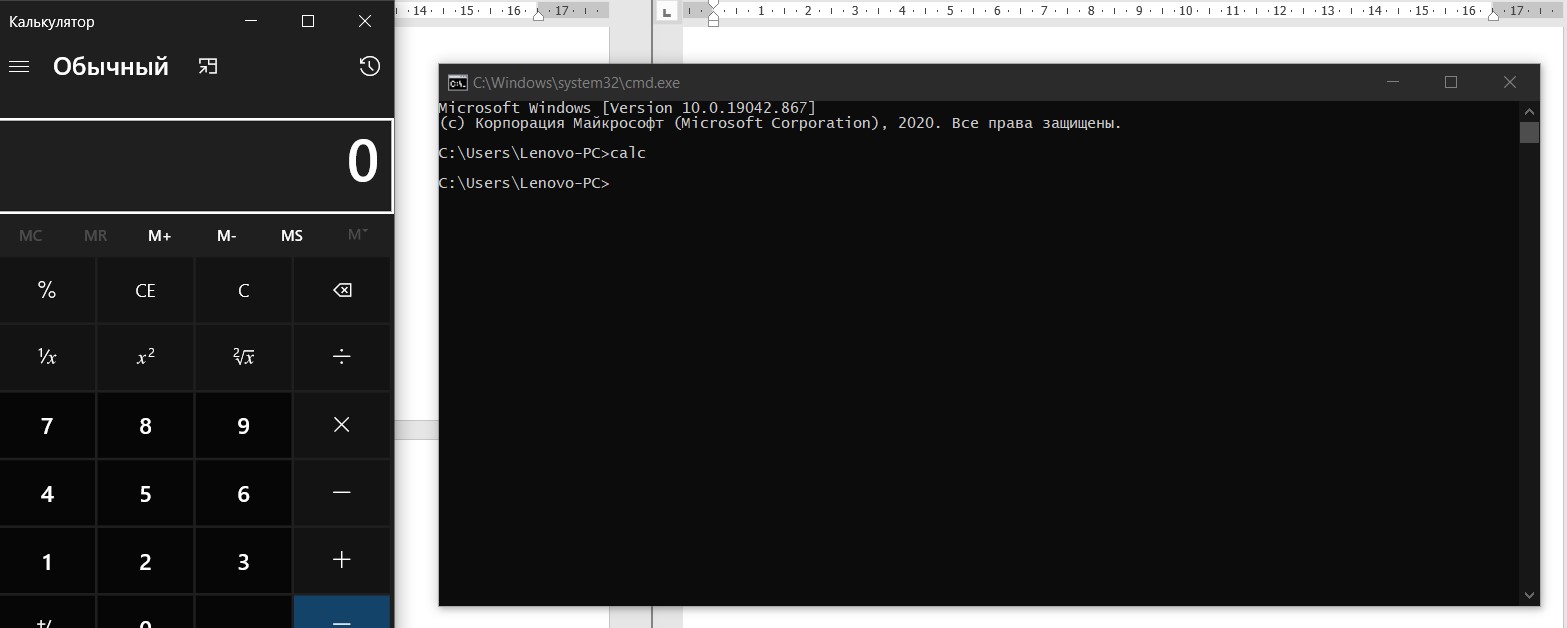
Итоговое созданное правило

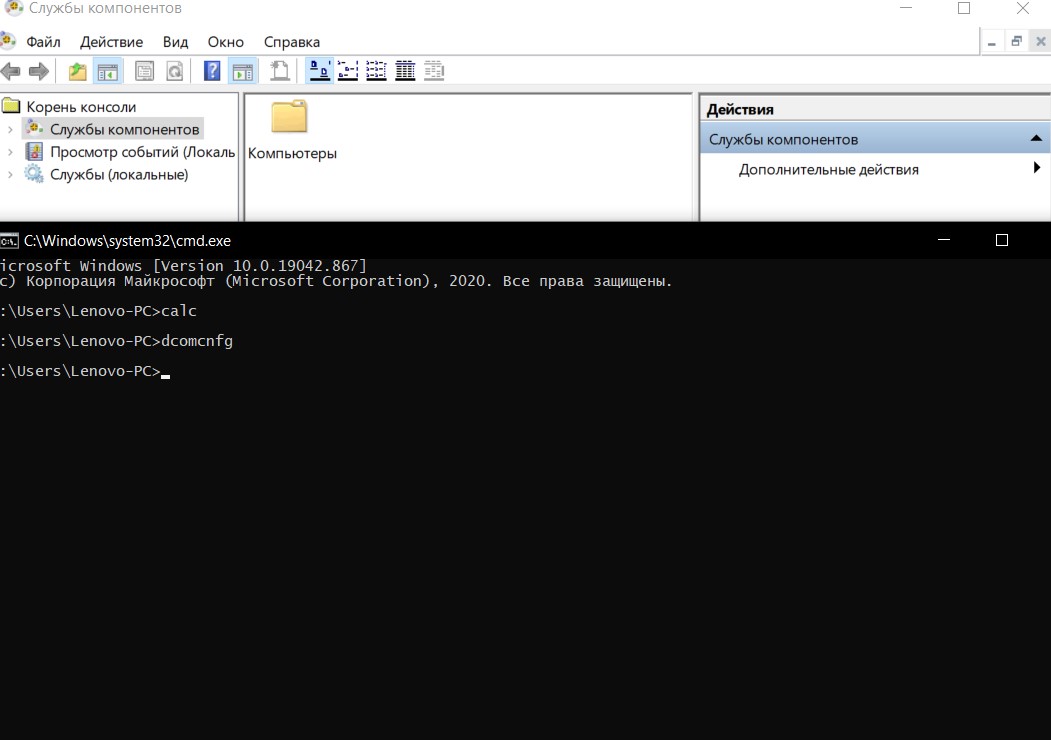


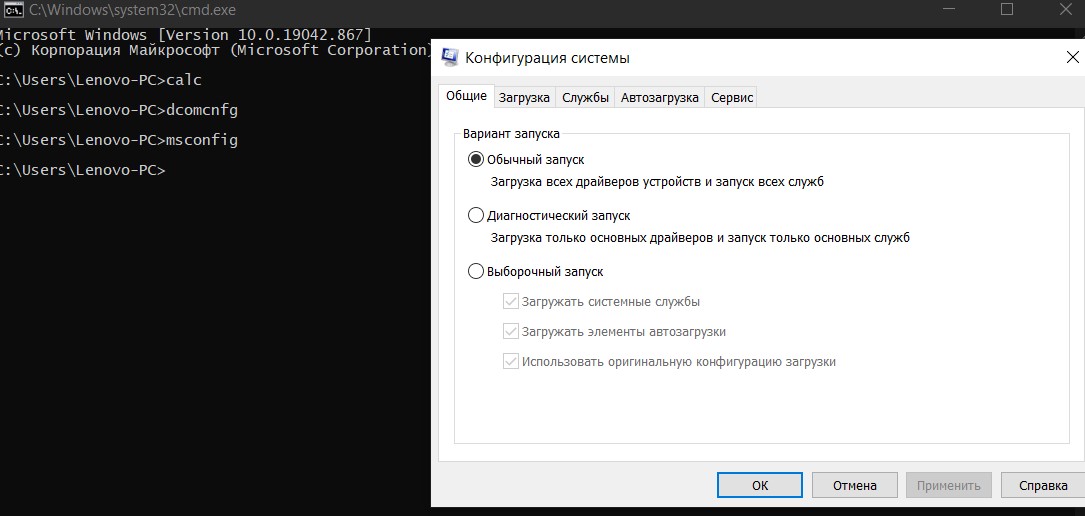




Правило для исходящих, его создание (разрешение)







Три вывода с помощью командной строки

Вывод: в ходе практической работы я научился работать с Брандмауэром Windows.

**Практическое занятие №5**

**Тема «Криптографическая защита информации»**

Цель: овладение основными криптографическими алгоритмами симметричного шифрования

Задание 1

Шкабров Данила Сергеевич

**Шифр Цезаря:** Ынгбусе Жгрлог Фзуёззелъ (ключ 3)

Исходный алфавит: А Б В Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я

Шифрованный: Г Д Е Ё Ж З И Й К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ъ Ы Ь Э Ю Я А Б В

**Шифр Трисемуса:**

Ключевое слово: защита

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| з | а | щ | и | т | б | в |
| г | д | е | ж | й | к | л |
| м | н | о | п | р | с | у |
| ф | х | ц | ч | ш | ъ | ы |
| ь | э | ю | я | . | , |  |

Итог: .сдкшцлцндхжудъошмоолжя

**Шифр Плейфера:**

Ключевое слово: защита

|  |  |  |  |
| --- | --- | --- | --- |
| з | а | щ | и |
| т | б | в | г |
| д | е | ж | и |
| к | л | м | н |
| о | п | р | с |
| у | ф | х | ц |
| ч | ш | ъ | ы |
| ь | э | ю | я |

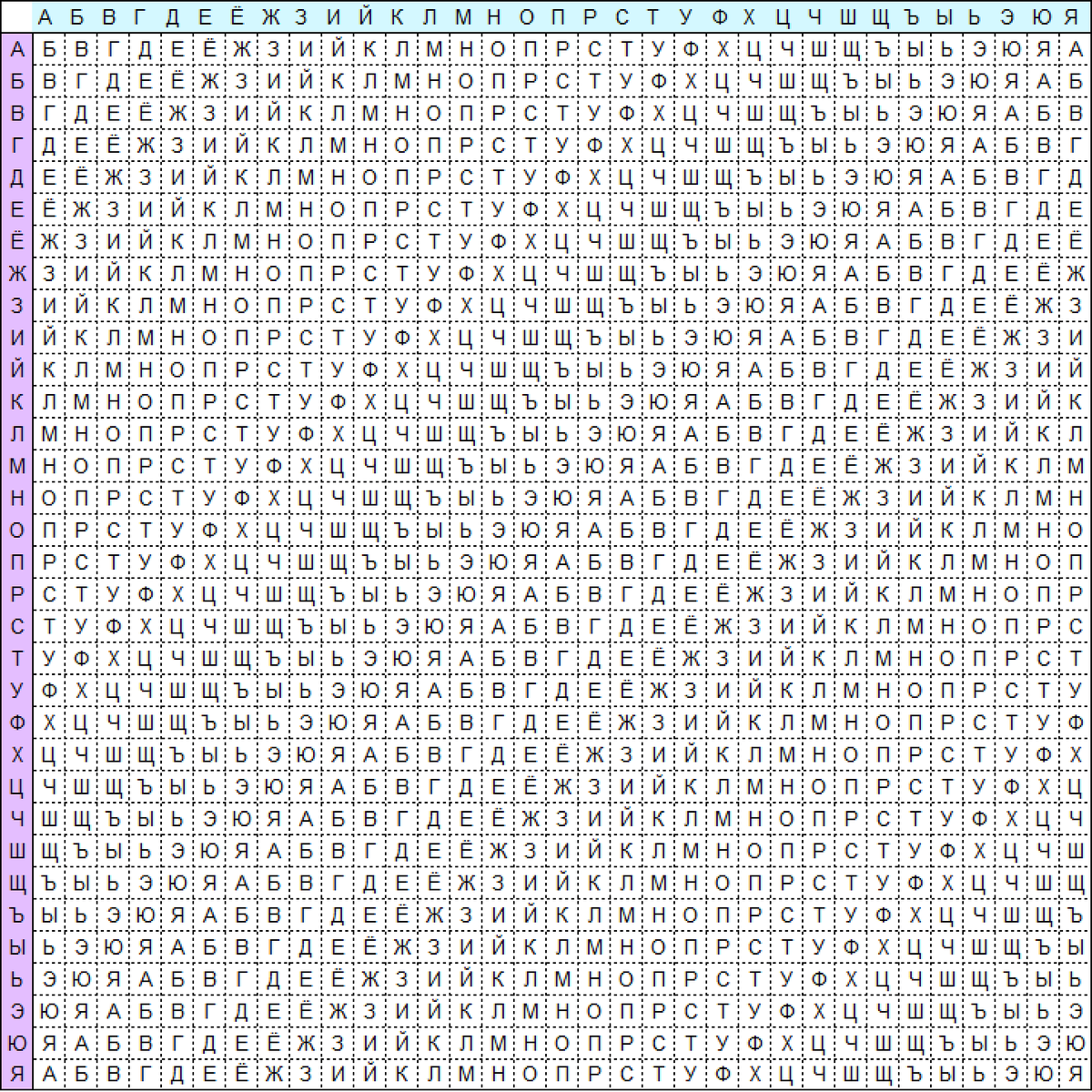
Шк аб ро вд ан ил ас ер ге ев ич

Итог: Лчбшостжлиенпипжиббжды

**Шифр Вижинера:**

Шкабровданиласергеевич

Ключевое слово: защита



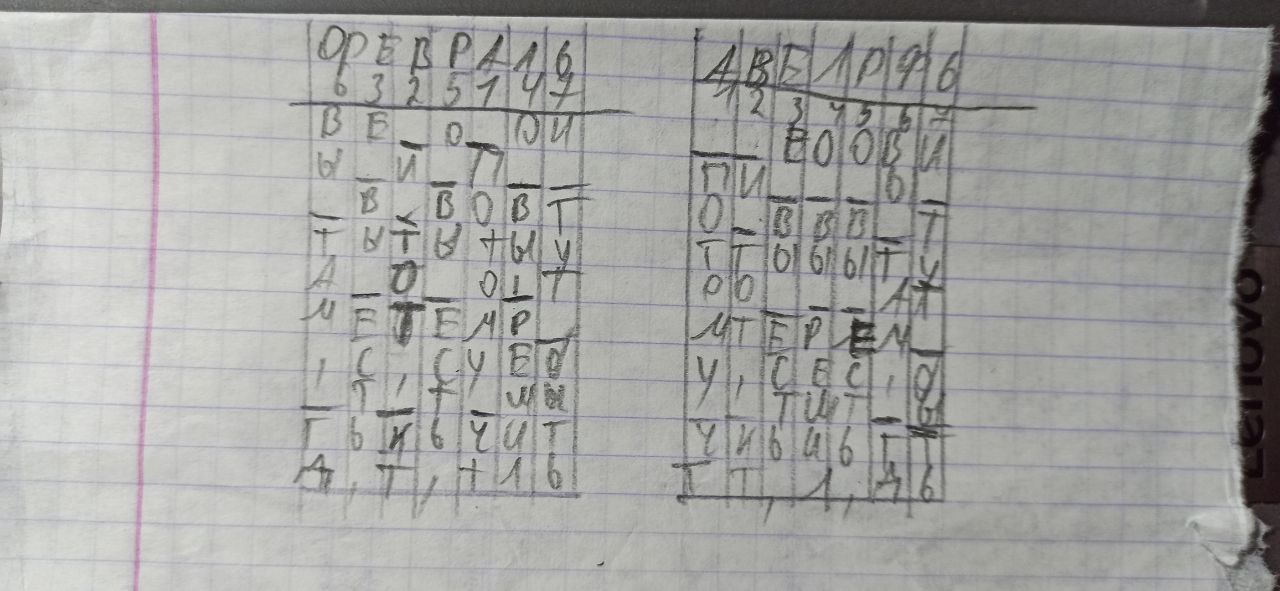
Итог: Блъкдпкезчьмитяъцёнгб

Задание 2

Расшифровать с помощью **Одиночной перестановки по ключу.**

**Ключ – ФЕВРАЛЬ Таблица 10х7**

**\_\_еоовипи\_\_\_ы\_о\_ввв\_тттыыытуоо\_\_\_атмтерем\_у,сес,б\_\_тшт\_ычкьиьгттт,л,дь**



*Решение*

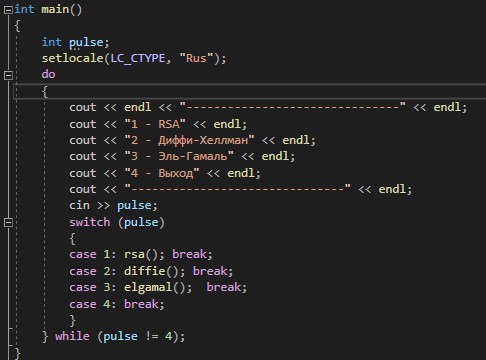
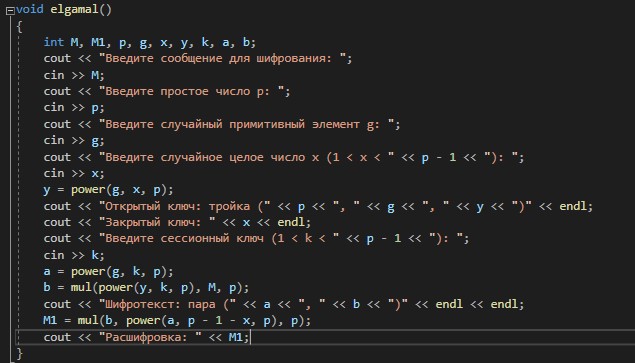
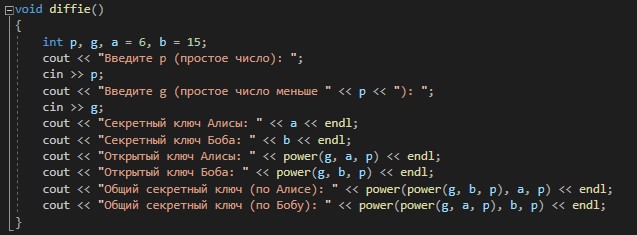
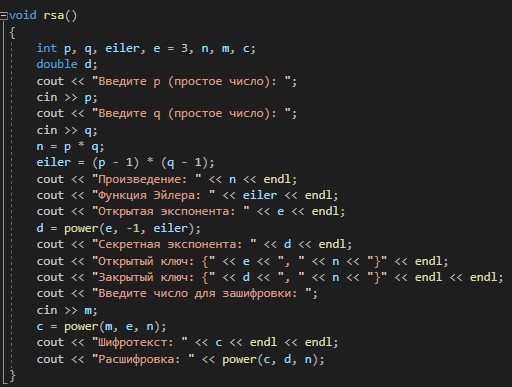
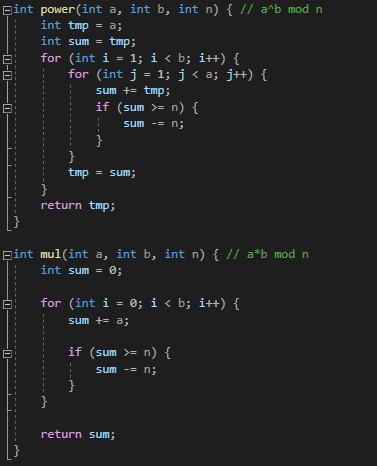
Ответ: Вы там, где вы есть, и тот, кто вы есть, потому что вы решили тут быть

Вывод: в ходе практической работы я овладел основными криптографическими алгоритмами симметричного шифрования

**Практическое занятие №6 (код)**

**Тема «Криптографическая защита информации»**

Цель: Овладение основными криптографическими алгоритмами асимметричного шифрования.

****

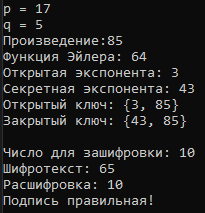
Вывод: в ходе практической работы я изучил и закрепил процесс работы алгоритмов RSA, Диффи-Хеллмана и Эль-Гамаля и реализовал их**.**

**Практическое занятие №7**

**Тема «Криптографическая защита информации»**

Цель: изучить и закрепить умение реализации ЭЦП на примере RSA**.**

Ход работы:



Код функции:

void var1()

{

int p = 17, q = 5, eiler, e = 3, n, m1 = 10, m2, c, d, s;

cout << "p = " << p << endl;

cout << "q = " << q << endl;

n = p \* q;

eiler = (p - 1) \* (q - 1);

cout << "Произведение:" << n << endl;

cout << "Функция Эйлера: " << eiler << endl;

cout << "Открытая экспонента: " << e << endl;

/\* d = power(e, -1, eiler); \*/ d = 43;

cout << "Секретная экспонента: " << d << endl;

cout << "Открытый ключ: {" << e << ", " << n << "}" << endl;

cout << "Закрытый ключ: {" << d << ", " << n << "}" << endl << endl;

cout << "Число для зашифровки: " << m1 << endl;

c = power(m1, e, n);

cout << "Шифротекст: " << c << endl;

cout << "Расшифровка: " << power(c, d, n) << endl; // power c d n

s = power(m1, d, n); // power m1 d n

m2 = power(s, e, n); // power s e n

if (m1 == m2)

{

cout << "Подпись правильная!" << endl;

}

else

{

cout << "Подпись некорректная" << endl;

}

}

Контрольные вопросы:

1. Дайте определение понятию "электронная цифровая подпись".

Электронная цифровая подпись – реквизит электронного документа, предназначенный для защиты данного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа ЭЦП и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе.

1. Объясните какой порядок использования ключей (открытый; закрытый) при отправке и проверке ЭЦП.

При создании цифровой подписи по классической схеме отправитель:

* применяет к исходному сообщению T хеш-функцию h(T) и получает хеш-образ r сообщения;
* вычисляет цифровую подпись s по хеш-образу r с использованием своего закрытого ключа;
* посылает сообщение T вместе с цифровой подписью s получателю.

Получатель, отделив цифровую подпись от сообщения, выполняет следующие действия:

* применяет к полученному сообщению T хеш-функцию h(T) и получает хеш-образ r сообщения;
* расшифровывает хеш-образ r’ из цифровой подписи s с использованием открытого ключа отправителя;
* проверяет соответствие хеш-образов r и r’ и если они совпадают, то отправитель действительно является тем, за кого себя выдает, и сообщение при передаче не подверглось искажению.

1. Перечислите специальные схемы ЭЦП.

Кроме классической схемы ЭЦП различают еще несколько специальных:

* схема "конфиденциальной" (неотвергаемой) подписи – подпись не может быть проверена без участия сгенерировавшего ее лица;
* схема подписи "вслепую" ("затемненной" подписи) - отправитель не знает подписанного им сообщения;
* схема "мультиподписи" - вместо одного отправителя сообщение подписывает группа из нескольких участников;
* схема "групповой" подписи - получатель может проверить, что подписанное сообщение пришло от члена некоторой группы отправителей, но не знает, кем именно из членов группы оно подписано.

Вывод: в ходе практической работы я изучил и закрепил умение реализации ЭЦП на примере RSA**.**

**Практическое занятие №8**

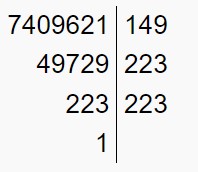
**Тема «Криптографическая защита информации»**

Цель: получение основных сведений из курса теории чисел

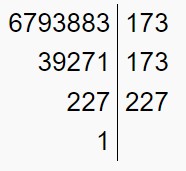
Вариант 15

1.Найти канонические разложения чисел а и b.

а = 7409621, b = 6793883



223\*223\*149 = 7409621



173\*173\*227 = 6793883

2. Найти НОД пользуясь a) алгоритмом Евклида, б) разложением чисел на простые множители.

а) Нужно отсортировать числа в порядке возрастания:**(**67938837409621**)**

Возьмем наименьшее число **(**6793883**)** как делитель

Выполним вычисления для операции по модулю оставшегося числа и делителя:

7409621mod 6793883= 615738

Получаем все остатки и делитель и сортируем их в порядке возрастания. Также удаляем все повторяющиеся номера. Тогда наш набор чисел: 615738 6793883

Имеется наименьший делитель из оставшихся чисел: 1. Следовательно, НОД(6793883; 7409621) является:**1**

б) Разложим числа на простые множители и подчеркнем общие множители чисел:

7409621 = 223\*223\*149

6793883 = 173\*173\*227

Общие множители чисел: 1

НОД (7409621; 6793883) = 1

3. С помощью расширенного алгоритма Евклида найти целые u, v, удовлетворяющие соотношению Безу: au + bv = НОД.

*au* + *bv =* 7409621*\* u +* 6793883*\* v =* НОД (7409621; 6793883) = 1

*u* = -2199628 *v* = 2398983

7409621*\** (-2199628) *+* 6793883 *\** 2398983*=* НОД (7409621; 6793883) = 1

6. Найти остаток от деления 20052003 на 17 (Вариант 2).

2005 делится на 17 с остатком 16. 20052 делится на 17 с остатком 1. 20053 делится на 17 с остатком 16. Получили один из предыдущих остатков, значит «зациклились». Число 20053 дает тот же остаток деления на 17, что и 2005. Значит, длина цикла равна 2. Число 20052003 дает тот же остаток от деления на 7, что и 2005, то есть 16.

Вывод: в ходе практической работы я получил основные сведения из курса теории чисел.

**Практическое занятие №9**

**Тема «Авторское право и смежные права»**

Цель работы: изучить основные положения авторского права и смежных прав.

Контрольные вопросы:

1. На какие объекты распространяется авторское право?

Авторское право распространяется на произведения науки, литературы и искусства, являющиеся результатом творческой деятельности, независимо от назначения и достоинства произведения, а также от способа его выражения

1. Что относится к личным неимущественным (моральным) правам?

Личные неимущественные права:

* признаваться автором произведения (право авторства);
* использовать или разрешать использовать произведение под подлинным именем автора, псевдонимом либо без обозначения имени, т.е. анонимно (право на имя);
* обнародовать или разрешать обнародовать произведение в любой форме (право на обнародование), включая право на отзыв;
* право на защиту произведения, включая его название, от всякого рода искажении или любого иного посягательства, способных нанести ущерб чести и достоинству автора (право на защиту репутации автора).

1. Что относится к личным имущественным правам?

Имущественные права (исключительное право осуществлять или разрешать осуществлять следующие действия):

* воспроизведение произведения;
* распространение оригинала или экземпляров произведения посредством продажи или иной передачи права собственности;
* прокат оригиналов или экземпляров компьютерных программ, баз данных, аудиовизуальных произведений, нотных текстов музыкальных произведений и произведений, воплощенных в фонограммах;
* импорт экземпляров произведения;
* публичный показ оригинала или экземпляра произведения;
* публичное исполнение произведения;
* передачу произведения в эфир;
* иное сообщение произведения для всеобщего сведения;
* перевод произведения на другой язык;

переделку или иную переработку произведения.

1. Каковы особенности авторского права на составные произведения?

Авторское право на составные произведения:

* Автору сборника и других составных произведений (составителю) принадлежит авторское право на осуществленные им подбор и распоряжение материалов как результат творческого труда (составительство).
* Составитель пользуется авторским правом при условии соблюдения им прав авторов каждого из произведений, включенных в составное.
* Авторы произведений, включенных в составное произведение, вправе использовать свои произведения независимо от составного произведения, если иное не предусмотрено авторским договором.
* Авторское право составителя не препятствует другим лицам осуществлять самостоятельный подбор и расположение тех же материалов для создания своих составных произведений.
* Лицу, выпускающему в свет энциклопедии, энциклопедические словари, периодические и продолжающиеся сборники научных трудов, газеты, журналы и другие периодические издания, принадлежат исключительные права на использование таких изданий в целом. Это лицо вправе при любом использовании таких изданий указывать свое наименование или требовать такого указания.
* Авторы произведений, включенных в такие издания, сохраняют исключительные права на использование своих произведений независимо от издания в целом, если иное не предусмотрено авторским договором.

1. Каков срок действия авторского права?

Право авторства, право на имя и право на защиту репутации автора охраняются бессрочно. Имущественные права действуют в течение всей жизни автора (соавторов) и 50 лет после его (последнего соавтора) смерти.

1. Кто является субъектом авторского права?

Субъектом авторского права, как правило, является гражданин, творческим трудом которого создано произведение науки, литературы или искусства. Им может быть и гражданин, не достигший восемнадцатилетнего возраста и душевнобольной. Так, авторские права детей, представленные на смотры или выставки детской или юношеской самодеятельности и т.д. защищаются авторским правом.

Но недееспособные, став субъектами авторского права, не имеют права самостоятельно совершать какие-либо сделки, связанные с использованием авторского права. Несовершеннолетние в возрасте от 14 до 18 лет могут самостоятельно осуществлять авторские права на свои произведения.

1. Что такое авторский договор?

Авторский договор — это соглашение двух или более лиц, направленное на установление, изменение и прекращение взаимных прав и обязанностей, касающихся имущественных и связанных с ними личных неимущественных прав.

1. Наиболее распространенные виды авторских договоров?

Наиболее распространенные виды авторского договора:

* Издательский (издание и переиздание любых произведений, которые могут быть зафиксированы на бумаге, т.е. произведений литературы (научных, художественных, учебных и т.п.), драматических, сценарных, музыкальных произведений, произведений изобразительного искусства)
* Постановочный (основным способом использования произведения является его публичное исполнение)
* Сценарный (договор, который регламентирует отношения, связанные с использованием текста, по которому снимается кинофильм, телефильм, делается радио- или телепередача, проводится массово-зрелищное мероприятие)
* художественного заказа (опосредует отношения, связанные с созданием произведений изобразительного искусства в целях их публичной демонстрации)

- об использовании в промышленности неопубликованного произведения декоративно-прикладного искусства.

1. Основные составляющие авторского договора?

Авторский договор должен предусматривать способы использования произведения (конкретные права, передаваемые по данному договору)

При отсутствии в авторском договоре условия о сроке передачи прав договор может быть расторгнут автором по истечении пяти лет с даты его заключения

При отсутствии в авторском договоре условия о территории, на которую распространяется действие этого права на указанный срок, действие передаваемого по договору права ограничиваются территорией РБ.

Размер и порядок начисления авторского вознаграждения за использование произведений литературы, науки и искусства устанавливаются в авторских договорах и (или) в договорах на право использования произведений, которые пользователи обязаны заключить с иными правообладателями либо с организациями, управляющими имущественными правами авторов.

Вознаграждение определяется в авторском договоре в виде процента от дохода за соответствующий способ использования произведения, или в виде твердо зафиксированной суммы, или иным образом.

Вывод: в ходе практической работы я изучил основные положения авторского права и смежных прав.

**Практическое занятие №10**

**Тема «Составление и оформление заявок на объекты промышленной собственности»**

Цель работы: овладеть навыками составления и оформления заявок на объекты промышленной собственности.

Контрольные вопросы:

1. Основные составляющие описания изобретения?

* область техники, к которой относится изобретение;
* уровень техники;
* сущность изобретения;
* перечень фигур чертежей, если они прилагаются с кратким указанием на то, что изображено на каждой из них. Если представлены иные материалы, поясняющие сущность изобретения, то перечисляют их;
* сведения, подтверждающие возможность осуществления изобретения.

1. Правила оформления описания изобретения?

Описание начинается с названия изобретения и указания индекса или индексов рубрики действующей редакции международной патентной классификации, к которой относится заявляемое изобретение. Названия разделов в тексте описания не указываются. Не допускается замена раздела «Описание» в целом или его части отсылкой к источнику, в котором находятся необходимые сведения. В разделе «Уровень техники» приводятся сведения об аналогах и прототипах.

1. Какие основные пункты должна содержать заявка на изобретение?

Заявка должна содержать документы:

* заявление о выдаче свидетельства;
* депонируемые материалы, содержащие комплект одного из следующих видов материалов: фотографии фотошаблонов; сборочный Топологический чертеж; послойные топологические чертежи; фотографии каждого слоя топологии;
* образцы ИМС с данной топологией в случае использования ее до даты подачи заявки;
* реферат;
* доверенность (в случае подачи через патентного поверенного).

1. Основные документы, необходимые для подачи заявки на изобретения?

Заявка подается в трех экземплярах и должна содержать:

* заявление о выдаче патента (типовой бланк);
* описание изобретения, раскрывающее его с полнотой достаточной для осуществления изобретения;
* формулу изобретения, выражающую его сущность и полностью основанную на описании;
* чертежи и иные материалы, если они необходимы для понимания сущности изобретения;
* реферат;
* доверенность в случае подачи заявки патентным поверенным.

1. ОТЛИЧИЯ заявок на охранные документы различных объектов промышленной собственности?

*Заявка на изобретение:*

Заявка на выдачу патента на изобретение подается автором изобретения, нанимателем, если изобретение служебное. Заявка подается в трех экземплярах. Вместе с заявкой или не позднее 2-х месяцев с даты ее подачи в одном экземпляре предоставляется документ, подтверждающий уплату пошлины в установленном размере.

*Заявка на выдачу патента:*

В данном разделе необходимо указать состав заявки, сколько экземпляров заявки необходимо подавать в патентный орган, а также на каких языках оформляется заявка. Временная правовая охрана заявленному изобретению предоставляется с даты публикации заявки до даты публикации сведений о патенте. Заявку на полезную модель преобразовать в заявку на изобретение возможно до даты получения решения о выдаче патента на полезную модель.

*Заявка на полезную модель:*

Заявка на полезную модель должна относиться к одной полезной модели или группу полезных моделей, связанных между собой так, что они образуют единый творческий замысел. До даты получения заявителем решения о выдаче патента на полезную модель, а в случае принятия решения об отказе в выдаче патента - до момента истечения срока его обжалования, возможно преобразование заявки на полезную модель в заявку на изобретение. Патент на полезную модель действует в течение пяти лет, считая с даты подачи заявки в патентный орган.

1. На какие ОПС выдаются патенты?

Патентно-лицензионная деятельность, регистрация объектов интеллектуальной собственности (ОИС), изобретения, полезные модели, промышленные образцы, товарные знаки и знаки обслуживания, топологии интегральных микросхем, компьютерные программы, оценка объектов интеллектуальной собственности (ОИС), процедура получения охранных документов.

1. На какие ОПС выдаются свидетельства?

Топологии интегральной микросхемы.

Вывод: в ходе практической работы я овладел навыками составления и оформления заявок на объекты промышленной собственности.

**Практическое занятие №11**

**Тема «Патентный поиск»**

Цель работы: изучить виды, содержание и порядок проведения патентных исследований.

**Теоретическая часть**

Целью патентных исследований является определение уровня техники, который используется для проверки соответствия заявленного изобретения условиям патентоспособности «новизна» и «изобретательский уровень».

Патентное исследование проводится на основании формулы изобретения с учетом описания и чертежей, если они имеются, а также с учетом изменений формулы изобретения, принятых во внимание при рассмотрении заявки.

При определении уровня техники общедоступными считаются сведения, содержащиеся в источниках информации, с которыми любое лицо может ознакомиться сами либо о содержании которых ему может быть законным путем сообщено.

*Международные классификаторы*

Для обеспечения единообразия в международном масштабе распределения патентных документов, а также упрощения поиска необходимой патентной документации применяются специально разработанные патентные классификаторы.

**Международная патентная классификация (МПК)**, принятая в соответствии со Страсбургским соглашением 1971 года, предусматривает создание единой системы классификации, охватывающей патенты на изобретения, включая опубликованные патентные заявки, авторские свидетельства, полезные модели и свидетельства о полезности. Аббревиатура **«МПК»** является общепринятым обозначением Международной патентной классификации.

**Международная классификация промышленных образцов (МКПО)** была принята 8 октября 1968 года дипломатической конференцией в г. Локарно (Швейцария), на которую были приглашены все страны-участницы Парижской конвенции по охране промышленной собственности.

**Международная классификация товаров и услуг (МКТУ)** в соответствии с Ниццким соглашением от 15 июня 1957 г., отражая единую классификацию товаров и услуг для регистрации товарного знака, позволяет c максимальной достоверностью идентифицировать и, соответственно, классифицировать товар или услугу с обеспечением их единообразного восприятия всеми заинтересованными лицами.

**Универсальная десятичная классификация** **(УДК),** первое сводное издание которой, вышло в 1905 г. в Брюсселе, получила широкое применение в качестве единой системы классификации информационных материалов в области естественных и технических наук. Ее применение позволяет обеспечить единообразие в организации справочно-информационных фондов в органах научно-технической информации, научных и технических библиотеках страны.

*Международная патентная классификация (МПК)*

**МПК** является средством для единообразного в международном масштабе классифицирования патентных документов, позволяет эффективно осуществлять поиск патентных документов с целью установления новизны и оценки вклада изобретателя в заявленное техническое решение (включая оценку технической прогрессивности и полезного результата).

**МПК**, кроме того, является:

* инструментом для упорядоченного хранения патентных документов, что облегчает доступ к содержащейся в них технической и правовой информации;
* основой для избирательного распределения информации среди потребителей патентной информации;
* основой для определения уровня техники в отдельных областях;
* основой для получения статистических данных в области промышленной собственности, что в свою очередь позволит определять уровень развития различных отраслей техники.

**МПК** охватывает все области знаний, объекты которых могут подлежать защите охранными документами. Иерархическая структура МПК выражается в разбивке всех областей знаний на несколько классификационных уровней. В нисходящем порядке эти уровни иерархии соответствуют разделам, классам, подклассам, основным группам и подгруппам.

По своей структуре МПК разделена на восемь основных разделов.

***Индекс раздела.*** Каждый раздел обозначен заглавной буквой латинского алфавита от **А** до **Н**.

***Заголовок раздела*** лишь приблизительно отражает его содержание. Разделы имеют следующие названия:

**A** – удовлетворение жизненных потребностей человека;

**B** – различные технологические процессы; транспортирование;

**C** – химия; металлургия;

**D** – текстиль; бумага;

**E** – строительство; горное дело;

**F** – механика; освещение; отопление; двигатели и насосы; оружие; боеприпасы; взрывные работы;

**G** – физика;

**H** – электричество.

***Содержание раздела***. В оглавлении к каждому разделу помещен перечень относящихся к нему *классов* и *подклассов*.

***Подраздел.*** Внутри разделов родственные классы условно объединяются в подразделы, которые не обозначаются индексами.

**Практическая часть**

В результате проведения исследовательских и проектно-конструкторских работ на промышленных предприятиях были разработаны методы испытания материалов. Для реализации этих методов предложены конструктивные решения приборов и приспособлений. В результате модернизации и совершенствования технологических процессов были предложены решения, позволяющие повысить качество и производительность выпускаемой продукции. Предполагается патентование разработки.

Необходимо выполнить экспертизу патентной чистоты разработанных конструктивных решений: методов испытания материалов и устройств для их осуществления; устройств и механизмов для реализации технологических процессов (рис. 1).

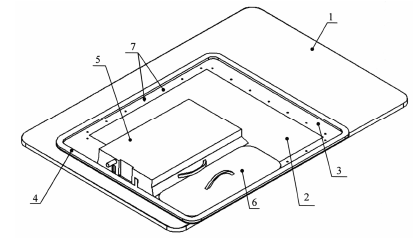
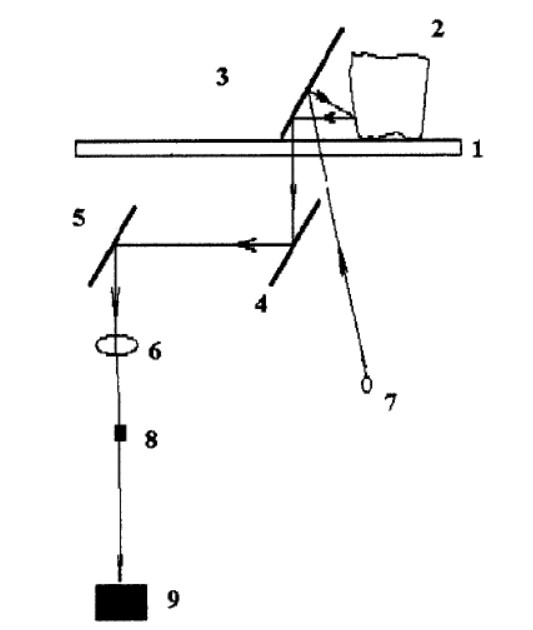


Рис. 1. Конструкция устройства пофрагментного сканирования графических документов

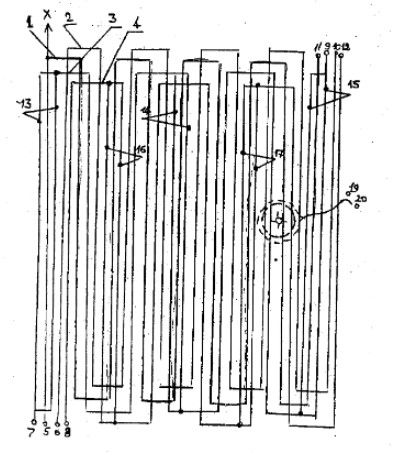
Для выявления патентной чистоты разработанного объекта промышленной собственности следует использовать следующий регламент поиска:

1. объект – устройство для пофрагментного сканирования графических документов*;*
2. страна поиска – *Республика Беларусь*;
3. источники информации – *патентные*;
4. ретроспективность – *5 лет*;
5. информационная база – *сайт национального центра интеллектуальной собственности* <https://bypatents.com/>

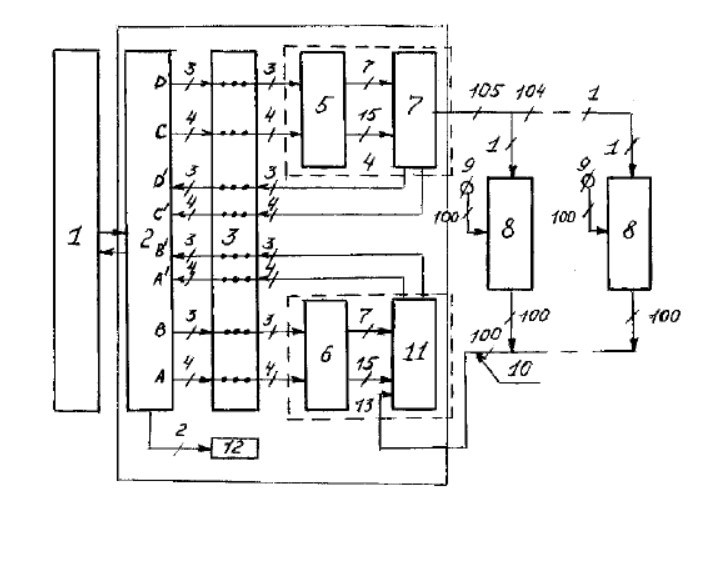
В итоге, проведем поиск по необходимым параметрам. Результаты, схожие по своему функционалу, представлены на рисунках 2-4.



# Рис. 2. Устройство для сканирования трехмерных объектов



# Рис. 3. Планшет для устройства считывания графической информации



# Рис. 4. Cистема сканирования информации с датчиков

Все данные по обнаруженным патентам-аналогам сводятся в соответствующую таблицу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охран-ного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Устройство пофрагментного сканирования графических документов | Патент РБ № U 1288  МПК [H03J 7/00](https://bypatents.com/patents/h03j-7-00) | Корхова Наталья Валерьевна, Ламбин Леонид Николаевич, Левин Генрих Моисеевич, Полонейчик Николай Михайлович, Токаревич Игорь Владиславович (BY), заявка № u 20030012 от 16.01.2003, опубл. 30.03.2004 | «Устройство для сканирования трехмерных объектов» | Не действует |
| Патент РБ №157  МПК [H03J 7/00](https://bypatents.com/patents/h03j-7-00) | [Алексеев Герт Иванович](https://bypatents.com/patents/alekseev-gert-ivanovich) (BY), заявка №1774356 от 08.11.1993, опубл. 30.09.1994 | «Планшет для устройства считывания графической информации» | Не действует |
| Патент РБ №3089  МПК [H04M 15/00](https://bypatents.com/patents/h04m-15-00), [H04M 15/18](https://bypatents.com/patents/h04m-15-18) | [Радивилов Николай Кириллович](https://bypatents.com/patents/radivilov-nikolajj-kirillovich) (BY), заявка №950264 от 29.05.1995, опубл. [30.12.1999](https://bypatents.com/1999/12/30) | «Cистема сканирования информации с датчиков» | Не действует |

Дальнейший анализ сущности обнаруженной патентной информации, выполняемой специалистами, позволяет определить наличие существенных отличий и возможность получения патента на изобретение или полезную модель.

Вывод: в ходе лабораторной работы я изучил виды, содержание и порядок проведения патентных исследований.

**Практическое занятие №12**

**Тема «Патентный поиск»**

Цель работы: изучить виды, содержание и порядок проведения патентных исследований.

**Практическая часть**

В результате проведения исследовательских и проектно-конструкторских работ на промышленных предприятиях были разработаны методы испытания материалов. Для реализации этих методов предложены конструктивные решения приборов и приспособлений. В результате модернизации и совершенствования технологических процессов были предложены решения, позволяющие повысить качество и производительность выпускаемой продукции. Предполагается патентование разработки.

Необходимо выполнить экспертизу патентной чистоты разработанных конструктивных решений. Проведем патентный поиск различной хоккейной амуниции.

Для выявления патентной чистоты разработанного объекта промышленной собственности следует использовать следующий регламент поиска:

1. объект – защита от повреждения во время спортивной игры хоккей, для минимизации травм;
2. страна поиска – *Республика Беларусь*;
3. источники информации – *патентные*;
4. ретроспективность – *5 лет*;
5. информационная база – *сайт национального центра интеллектуальной собственности:* [http://www.belgospatent.org.by](http://www.belgospatent.org.by/)

В итоге, проведем поиск по необходимым параметрам. Результаты, схожие по своему функционалу, представлены на рисунках 1-3.

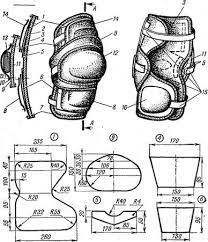


Рис. 1. Налокотники хоккейные

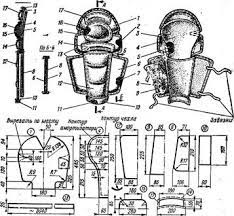


Рис. 2. Наколенники хоккейные (полевые)

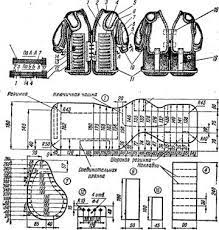


Рис. 3. Наколенники хоккейные (вратарские)

Все данные по обнаруженным патентам-аналогам сводятся в соответствующую таблицу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Предмет поиска (объект исследования, его составные части) | Страна выдачи, вид и номер охранного документа. Классификационный индекс | Заявитель (патентообладатель), страна. Номер заявки, дата приоритета, конвенционный приоритет, дата публикации | Название изобретения (полезной модели, промышленного образца) | Сведения о действии охранного документа или причина его аннулирования (только для анализа патентной чистоты) |
| Хоккейная амуниция | Патент РБ №7091  МПК 7 B 62D 21/08 | Корун Александр Владимирович (BY), Вротон Петр Иванович (BY), заявка №а20041227 от 2004.12.27, опубл. 2005.06.30 | «Налокотники хоккейные» | Не действует |
| Патент РБ №6655  МПК 7 B 60J 1/04 | Герасименя Николай Данилович (BY), заявка №а20010921 от 2001.09.21, опубл. 2003.03.30 | «Наколенники хоккейные (полевые)» | Не действует |
| Патент РБ №1351  МПК 6 B 60L 8/00 | Кореев Владимир Николаевич (BY), Головач Константин Эдуардович (BY), Боротон Виктор Андреевич (BY), заявка №2004 от 1994.06.27 | «Наколенники хоккейные (вратарские)» | Не действует |

Дальнейший анализ сущности обнаруженной патентной информации, выполняемой специалистами, позволяет определить наличие существенных отличий и возможность получения патента на изобретение или полезную модель.

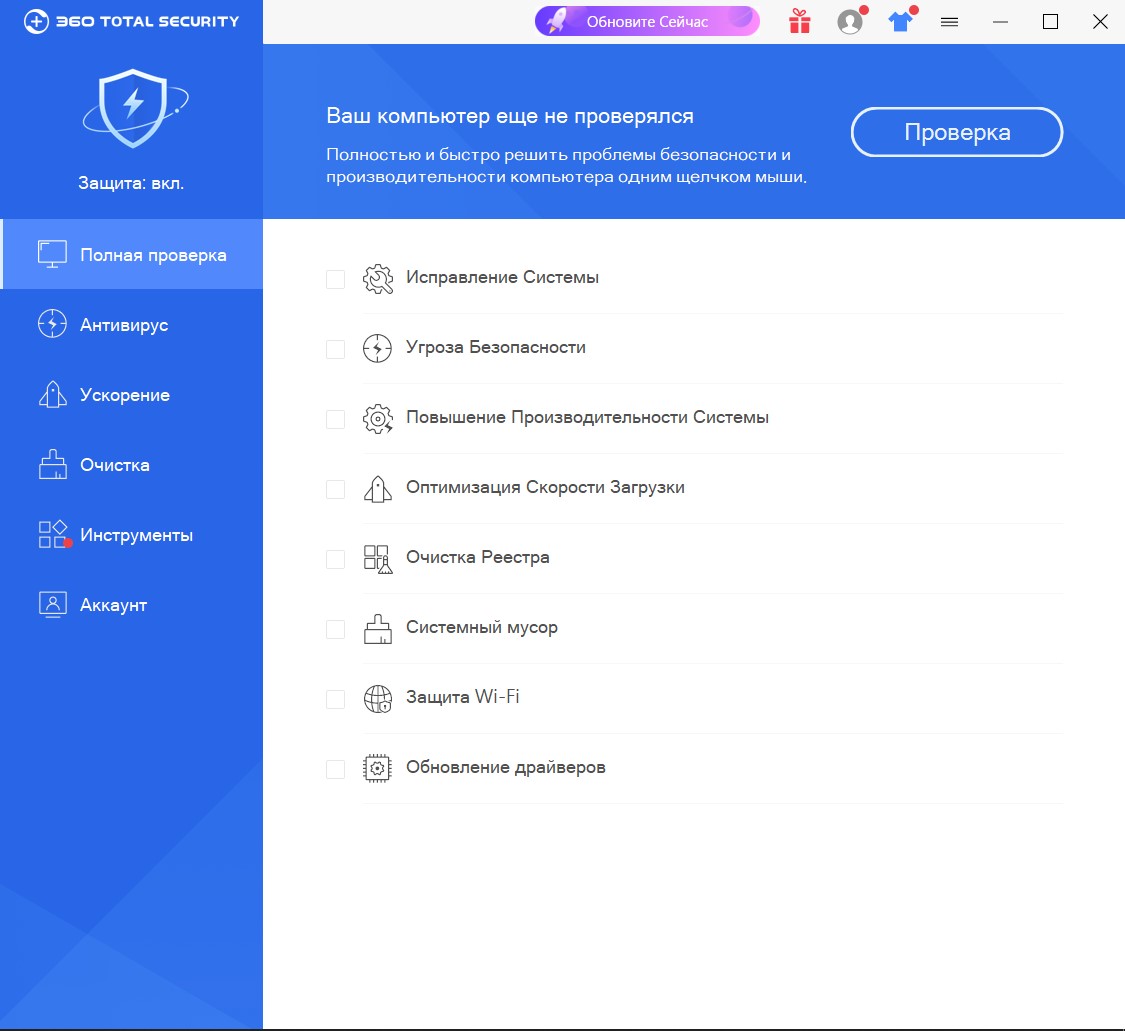
Вывод: в ходе лабораторной работы я изучил виды, содержание и порядок проведения патентных исследований.

**Практическое занятие №13**

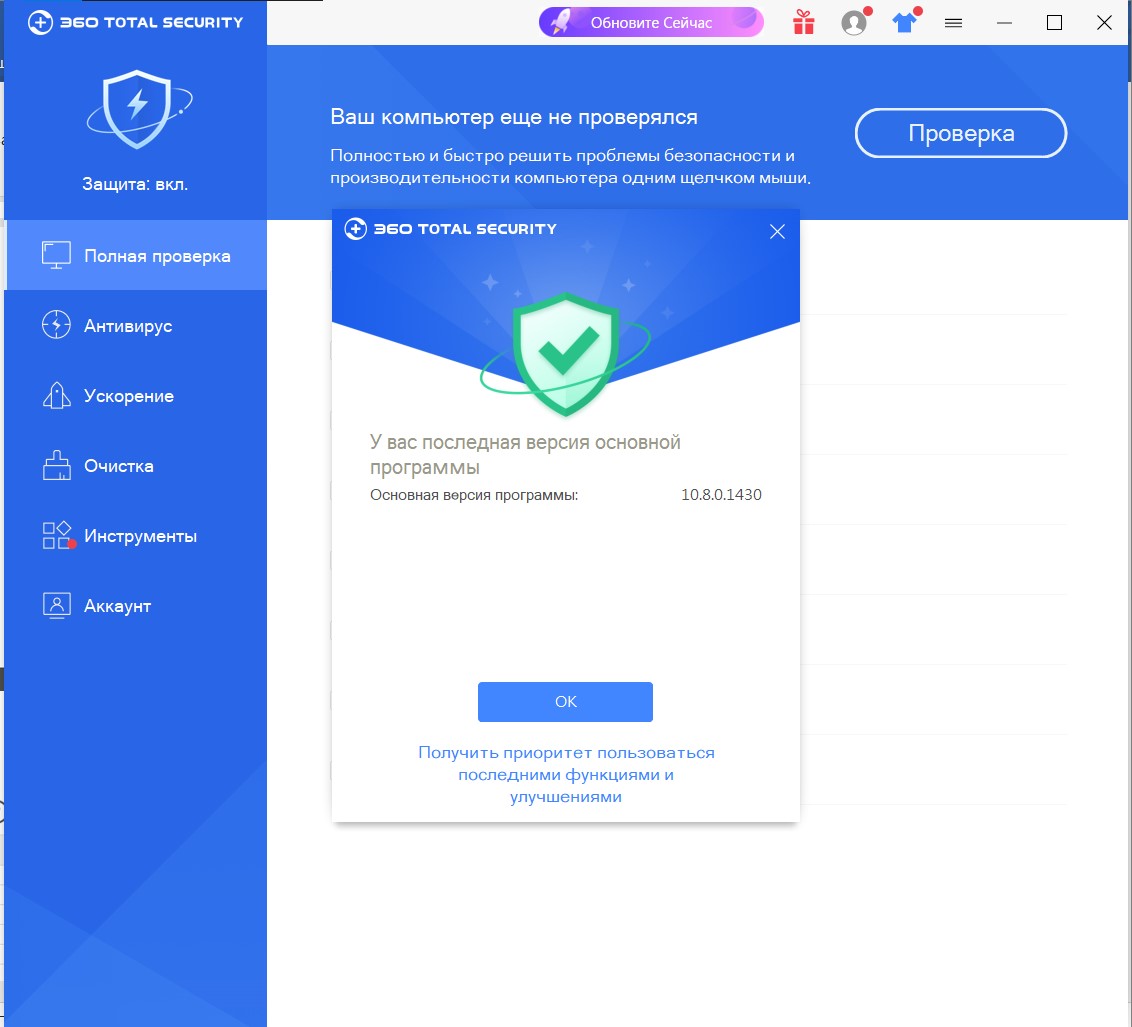
**Тема «Настройка антивирусов»**

Цель работы: овладение навыков настройки и использования антивирусов.

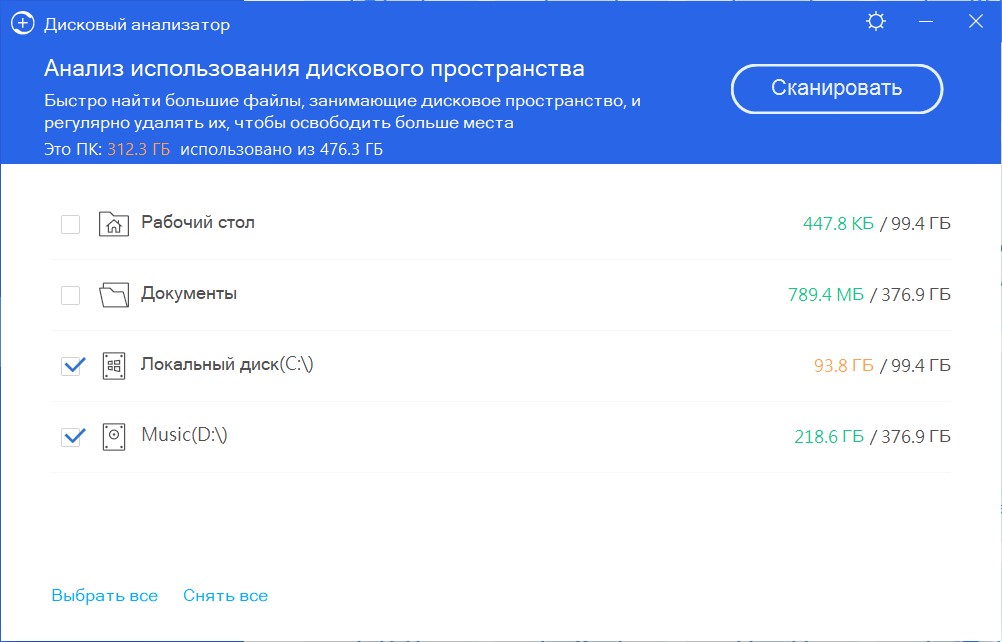
Рассмотрим антивирусное программное обеспечение 360 Total Security.



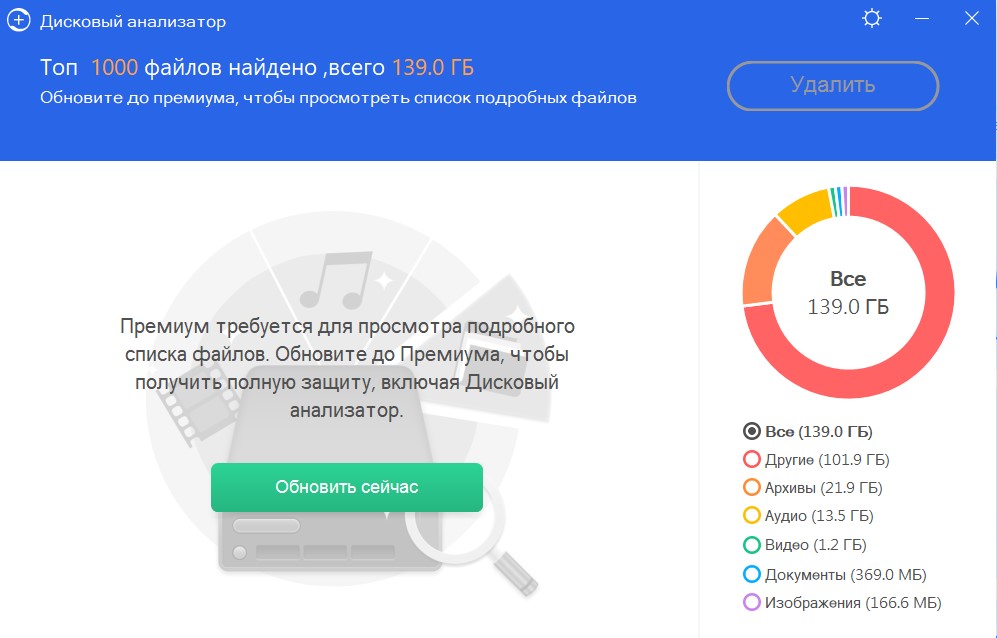
Основной экран настроек



Проверка установки обновлений



Проверка дисковых устройств



Сканирование дисков

Вывод: в ходе практической работы я овладел навыками настройки и использования антивирусов.

**Практическое занятие №14**

**Тема « Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки** [**System.Security.Cryptography**](https://docs.microsoft.com/ru-ru/dotnet/api/system.security.cryptography)**»**

Цель: изучить модель криптографии .NET Framework, Основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования

Контрольные вопросы:

1. Какие симметричные алгоритмы шифрования Вы знаете?

В симметричном шифровании один и тот же ключ используется как для шифрования, так и для дешифрования. В этом методе исходное сообщение преобразуется в нераспознаваемое сообщение, которое невозможно идентифицировать. Это преобразованное сообщение называется зашифрованным текстом. Это делается с помощью ключа и алгоритма шифрования. На принимающей стороне зашифрованный текст преобразуется обратно в исходное сообщение с использованием того же ключа и алгоритма дешифрования.

Поскольку обе стороны используют один и тот же ключ, симметричное шифрование намного быстрее. С другой стороны, ключ должен быть доступен для расшифровки сообщения. Поэтому для передачи ключа требуется защищенный канал. В целом, симметричное шифрование является простым методом и не требует много времени для завершения. RC4, AES, DES, 3DES - это некоторые распространенные алгоритмы симметричного шифрования.

1. Какие ассиметричные алгоритмы шифрования Вы знаете?

Асимметричное шифрование использует два ключа для шифрования и дешифрования. Эти два ключа называются закрытым ключом и открытым ключом. Он использует открытый ключ для шифрования и закрытый ключ для расшифровки. Открытый ключ доступен для стороны, которая хочет отправить сообщение. Закрытый ключ принадлежит владельцу сообщения. Сообщение, которое зашифровано открытым ключом и алгоритмом шифрования, может быть дешифровано с использованием алгоритма дешифрования и соответствующего закрытого ключа соответствующего открытого ключа.

В целом, асимметричное шифрование обеспечивает большую безопасность данных. С другой стороны, использование двух ключей делает асимметричное шифрование трудоемким и более сложным. Алгоритм Диффи-Хеллмана и RSA - это некоторые распространенные алгоритмы асимметричного шифрования.

1. Основное назначение библиотеки System.Security.Cryptography?

Предоставляет криптографические службы, включая безопасное кодирование и декодирование данных, а также множество других операций, таких как хэширование, генерация случайных чисел и проверка подлинности сообщений.

1. Влияет ли размер ключа на криптостойкость алгоритма?

Размер ключа измеряется в битах (двоичных разрядах). Чем он больше, тем, соответственно, больше времени необходимо на перебор возможных значений, но и тем продолжительнее работает алгоритм. Поэтому выбор оптимальной длины ключа — это вопрос баланса.

1. Назовите основные классы библиотеки System.Security.Cryptography?

Класс CSPParameters – содержит параметры, передаваемые поставщику служб шифрования (CSP), который выполняет криптографические вычисления.

Класс CspParameters представляет параметры, которые можно передавать управляемым криптографическим классам, использующим службы шифрования (CSP), с помощью интерфейса Microsoft Cryptography API (CAPI).

Класс RSACryptoServiceProvder - выполняет шифрование и дешифрование данных с помощью реализации асимметричного алгоритма RSA, предоставляемого поставщиком служб шифрования (CSP).

Структура RSAParameters - представляет стандартные параметры для алгоритма RSA (значения d, e, n, p, q и т.д.)

Класс RijndaelManaged – реализует симметричный алгоритм шифрования Rijndael. Поддерживаются ключи длиной 128, 192 и 256 бит.

Вывод: в ходе практической работы я изучил модель криптографии .NET Framework, основные классы и структуры данных.