


Министерство науки и высшего образования Российской Федерации
ФГБОУ ВО «Кубанский государственный технологический университет»
(ФГБОУ ВО «КубГТУ»)

Многоотраслевой институт подготовки и переподготовки специалистов
(МИППС)

Факультет: по работе со студентами ускоренного обучения по
индивидуальным учебным планам
Кафедра: компьютерных технологий и информационной безопасности
Направление подготовки: 09.03.04 Программная инженерия
Профиль: беспрофильный

КОНТРОЛЬНАЯ РАБОТА № 1
Вариант №2

по дисциплине Информационная безопасность программных систем
(наименование дисциплины)
Студент (ка) 3 курса, шифр 17-ЗКБс-ПР1, специальность 09.03.04
Фамилия Бабича 
Имя Михаила Отчество Михайловича
Дата поступления работы _____
Оценка _____ Рецензент Федоров С. Ю.
” ” _____ 20__ г. Подпись _____

Содержание

Теоретический вопрос	3
Практическое задание № 1	10
Практическое задание № 2.	14
Практическое задание № 3.	16
Список используемых источников	18

Теоретический вопрос

Вариант 2. Виды уязвимостей вычислительных сетей и их характеристика («buffer overflow», «SQL Injection», «format string», «Directory traversal», «Cross Site Scripting» и уязвимости программных реализаций стека TCP/IP).

Переполнение буфера (Buffer Overflow)— запись или чтение программой данных за пределами выделенного для этого в памяти буфера. Обычно возникает из-за неправильной работы с данными и памятью, при отсутствии жесткой защиты со стороны подсистемы программирования и ОС. Данный вид ошибок достаточно распространён и часто связан с опечатками при наборе. Существует также родственная ошибка - неполная обработка буфера (Buffer Underflow).

Ошибки Buffer Overflow и Buffer Underflow буфера часто приводят к использованию в программе неинициализированных данных и как следствие к её неопределённому поведению. Переполнение буфера также может стать причиной ошибки сегментации (Access Violation).

Так как большинство языков высокого уровня размещают данные программы в стеке процесса, смешивая их с управляющими данными, переполнение буфера является одним из наиболее распространённых способов взлома ПО, позволяя загрузить и выполнить произвольный машинный код от имени программы и с правами учетной записи запустившего её пользователя.

В таких распространённых языках, как C и C++, отсутствует встроенная проверка на границы чтения/записи данных. Это плата за возможность эффективной низкоуровневой работы с оперативной памятью. С другой стороны, практически все интерпретируемые языки и ЛТ среды (Java RTE, .NET Framework) имеют встроенную защиту от переполнения буфера.

Для предотвращения использования уязвимости переполнения буфера во время исполнения программы существуют системы защиты от

повреждения стека (Libsafe, StackGuard), системы защиты пространства исполняемого кода. Сложность же динамического обнаружения ошибок переполнения буфера связана с тем, что программа долгое время может работать стабильно, т.к. в неинициализированной памяти могут находиться приемлемые значения, а область перезаписываемой памяти может не использоваться. На этапе написания/отладки кода ошибки переполнения буфера и связанные с ними уязвимости могут быть обнаружены с помощью статического анализа.

SQL Injection

Structured Query Language (SQL) — это структурированный язык, используемый для взаимодействия с базами данных. Существует множество «диалектов» языка SQL, но сегодня, в основном, все они построены на основе стандарта SQL-92, один из ранних ANSI стандартов. Основным операционным блоком SQL — запрос (query), который является совокупностью выражений, которые обычно возвращают совокупность результатов (result set). SQL выражения могут изменять структуру баз данных (используя выражения языков определения данных — DDL) и управлять их содержанием (используя выражения языков манипулирования данными — DML). В данной работе, мы рассмотрим transact-SQL, использующийся в Microsoft SQL Server.

SQL-инъекции возможны в том случае, когда злоумышленник может вставить свой SQL-код в запрос (query), для управления данными, которые отправляются в приложение.

Обычное SQL выражение выглядит следующим образом:

```
select id, forename, surname from authors
```

Это выражение берет «id», «forename» и «surname» из колонок таблицы «authors» и возвращает все строки в таблице. Выборка может быть ограничена, определенным «автором», например:

```
select id, forename, surname from authors where forename = 'john' and  
surname = 'smith'
```

Необходимо отметить, что в данном запросе строковые литералы разделены одинарной кавычкой. Предполагается, что «forename» и «surname» являются данными, которые вводятся пользователем. В данном случае злоумышленник будет способен внести собственный SQL-запрос, путем добавления собственных значений в приложение. Например:

```
<source lang="html">
```

```
Forename: jo'hn
```

```
Surname: smith
```

Тогда выражение примет следующий вид:

```
select id, forename, surname from authors where forename = 'jo'hn' and  
surname = 'smith'
```

После того, как база данных попытается обработать подобный запрос будет возвращена следующая ошибка:

```
Server: Msg 170, Level 15, State 1, Line 1
```

```
Line 1: Incorrect syntax near 'hn'.
```

Причина ошибки будет заключаться в том, что введенная одиночная кавычка испортит структуру разделителей в запросе. Таким образом, база данных безуспешно попытается выполнить команду «hn», которая приведет к ошибке. В итоге, если злоумышленник введет в форму следующую информацию:

```
Forename: jo'; drop table authors--
```

```
Surname:
```

Таблица «authors» будет удалена,

format string

Использование уязвимостей класса format string представляет собой новую технологию атак на безопасность систем. Несмотря на то, что данная технология известна еще с сентября 1999, должное внимание сетевой общественности было на нее обращено только после появления публичного exploit'a remote root для wu-ftpd 2.6.0 в июле 2000.

В данной главе исследуется суть проблемы и обосновывается утверждение, что желание укоротить свою программу на 6 байт достаточно, чтобы программа (а в некоторых случаях и безопасность самой системы) была скомпрометирована.

В чем состоит суть проблемы?

Большинство дыр в безопасности являются следствием или ошибок конфигурации или лени. Ошибки класса `format string` в очередной раз подтверждают справедливость этого правила.

Достаточно часто в программах возникает необходимость ввода-вывода куда-либо строковых данных. В отличие от атак переполнения буфера для `format string` не важно, куда именно выводятся строковые данные - стандартный поток вывода, файл, промежуточный буфер. Пример:

```
printf("%s", str);
```

Однако программист может решить сэкономить время или 6 байт и написать так:

```
printf(str);
```

Думая о экономии места, программист отрывает потенциальную дыру в безопасности. Возможно, он будет удовлетворен, тем, что `printf` передается только один аргумент, который он просто хотел вывести в стандартный поток вывода. Однако, при разборе строки формата передаваемой фактическим аргументом в ней, в любом случае, будет производится поиск спецификаторов формата (`%d`, `%g...`). Если какой-либо из них будет обнаружен, то в стеке производится соответствующий поиск аргумента для этого спецификатора.

Directory traversal

Обход каталогов (или путь обход) заключается в эксплуатации недостаточной безопасности проверка / санитарные имен файлов входных поставляемого пользователя, таким образом, что символы, представляющие «траверс родительского каталога» передается на файловом API.

Цель этой атаки заключается в использовании соответствующего приложения, чтобы получить несанкционированный доступ к файловой системе. Эта атака эксплуатирует отсутствие безопасности (программа действует точно так, как это предполагается), в отличие от использования ошибки в коде.

Обход каталогов также известен как ../ (точка точки слэша) атака, каталог восхождения и возвраты. Некоторые формы этого нападения также канонизация атака.

Cross-Site Scripting

Cross-Site Scripting или XSS. Межсайтовый скриптинг (межсайтовое выполнение сценариев).

Наличие уязвимости Cross-site Scripting позволяет атакующему передать серверу исполняемый код, который будет перенаправлен браузеру пользователя. Этот код обычно создается на языках HTML/JavaScript, но могут быть использованы VBScript, ActiveX, Java, Flash, или другие поддерживаемые браузером технологии.

Переданный код исполняется в контексте безопасности (или зоне безопасности) уязвимого сервера. Используя эти привилегии, код получает возможность читать, модифицировать или передавать важные данные, доступные с помощью браузера. У атакованного пользователя может быть скомпрометирован аккаунт (кража cookie), его браузер может быть перенаправлен на другой сервер или осуществлена подмена содержимого сервера. В результате тщательно спланированной атаки злоумышленник может использовать браузер жертвы для просмотра страниц сайта от имени атакуемого пользователя. Код может передаваться злоумышленником в URL, в заголовках Методы и структура протокола HTTP запроса (Cookie, user-agent, refferer), значениях полей форм и т.д.

Существует три типа атак, приводящих к межсайтовому выполнению сценариев: non-persistent непостоянные (отраженные), persistent постоянные (сохраненные) и основанные на DOM. Основным отличием

между persistent и non-persistent является то, что в отраженном варианте передача кода серверу и возврат его клиенту осуществляется в рамках одного HTTP- запроса, а в хранимом - в разных.

Осуществление непостоянной атаки требует, чтобы пользователь перешел по ссылке, сформированной злоумышленником (ссылка может быть передана по email, ICQ и т.д.). В процессе загрузки сайта код, внедренный в URL или заголовки запроса будет передан клиенту и выполнен в его браузере.

Сохраненная разновидность уязвимости возникает, когда код передается серверу и сохраняется на нем на некоторый промежуток времени. Наиболее популярными целями атак в этом случае являются форумы, почта с Web-интерфейсом и чаты. Для атаки пользователю не обязательно переходить по ссылке, достаточно посетить уязвимый сайт.

Уязвимости программных реализаций стека TCP/IP

Если АС имеет подключение к сетям общего пользования, то могут быть реализованы сетевые атаки на нее. К сетям общего пользования на основе стека протоколов TCP/IP относится и Интернет, на примере которого мы будем рассматривать наиболее распространенные в настоящее время атаки. Сеть Интернет создавалась для связи между государственными учреждениями и университетом с целью оказания помощи учебному процессу.

На начальном этапе никто не мог предположить дальнейший масштаб его развития и интеграции в жизнь современного общества, в связи с чем вопросам безопасности не уделялось должного внимания. Как следствие, на данный момент стек обладает множеством уязвимостей, которыми с успехом пользуются злоумышленники для реализации атак. Уязвимости протоколов, входящих в стек TCP/IP обусловлены, как правило, слабой аутентификацией, ограничением размера буфера, отсутствием проверки корректности служебной информации и т.п.

Наименование протокола	Уровень <i>стека протоколов</i>	Наименование (характеристика) уязвимости	Содержание нарушения <i>безопасности информации</i>
FTP (<i>File Transfer Protocol</i>) – протокол передачи файлов по сети	Прикладной, представительный, сеансовый	<ul style="list-style-type: none"> – Аутентификация на базе <i>открытого текста</i> (пароли пересылаются в незашифрованном виде) – Доступ по умолчанию – Наличие двух открытых портов 	<ul style="list-style-type: none"> – Возможность <i>перехвата</i> данных учетной записи (имен зарегистрированных пользователей, паролей). – Получение удаленного доступа к хостам
telnet – протокол управления удаленным терминалом	Прикладной, представительный, сеансовый	Аутентификация на базе <i>открытого текста</i> (пароли пересылаются в незашифрованном виде)	<ul style="list-style-type: none"> – Возможность <i>перехвата</i> данных учетной записи (имен зарегистрированных пользователей, паролей). – Получение удаленного доступа к хостам
UDP – протокол передачи данных без установления соединения	Транспортный	Отсутствие механизма предотвращения перегрузок буфера	<ul style="list-style-type: none"> – Возможность реализации UDP-шторма. – В результате обмена пакетами происходит существенное снижение производительности сервера
ARP – протокол преобразования IP-адреса в физический адрес	Сетевой	Аутентификация на базе <i>открытого текста</i> (информация пересылается в незашифрованном виде)	Возможность перехвата трафика пользователя злоумышленником
RIP – протокол маршрутной информации	Транспортный	Отсутствие аутентификации управляющих сообщений об изменении маршрута	Возможность перенаправления трафика через хост злоумышленника
TCP – протокол управления передачей	Транспортный	Отсутствие механизма проверки корректности заполнения служебных заголовков пакета	Существенное снижение скорости обмена и даже полный разрыв произвольных соединений по протоколу TCP
DNS – протокол установления соответствия мнемонических имен и сетевых адресов	Прикладной, представительный, сеансовый	Отсутствие средств проверки аутентификации полученных данных от источника	<i>Фальсификация</i> ответа <i>DNS-сервера</i>
IGMP – протокол передачи сообщений о маршрутизации	Сетевой	Отсутствие аутентификации сообщений об изменении параметров маршрута	Зависание систем Win 9x/NT/2000
SMTP – протокол обеспечения сервиса доставки сообщений по электронной почте	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность подделывания сообщений электронной почты, а также адреса <i>отправителя сообщения</i>
SNMP – протокол управления маршрутизаторами в сетях	Прикладной, представительный, сеансовый	Отсутствие поддержки аутентификации заголовков сообщений	Возможность переполнения пропускной способности сети

Практическое задание № 1

Для каждого варианта практического задания № 1 необходимо описать настройку средства защиты информации и снять снимки с экрана.

Описать назначение и настройку VPN соединения сети

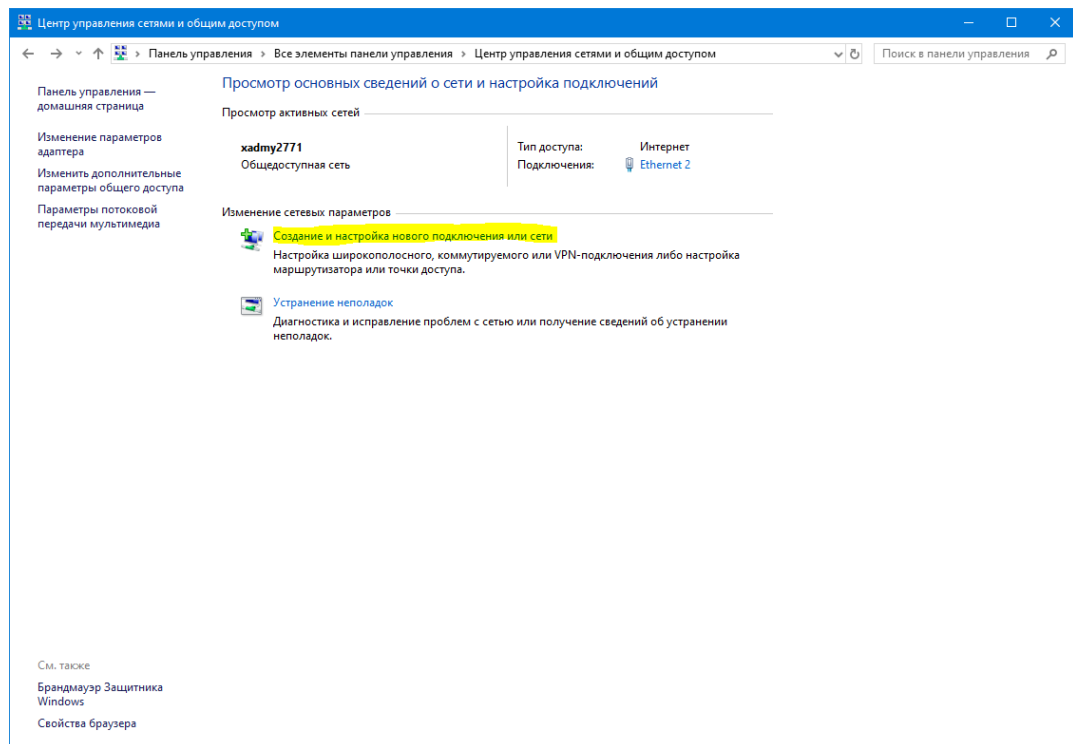
Виртуальная частная сеть (VPN) обеспечивает чрезвычайно надежное соединение частных сетей через Интернет. За счет этого удаленные компьютеры могут взаимодействовать друг с другом так, как если бы они находились в одной защищенной локальной сети.

Преимущества виртуальных частных сетей

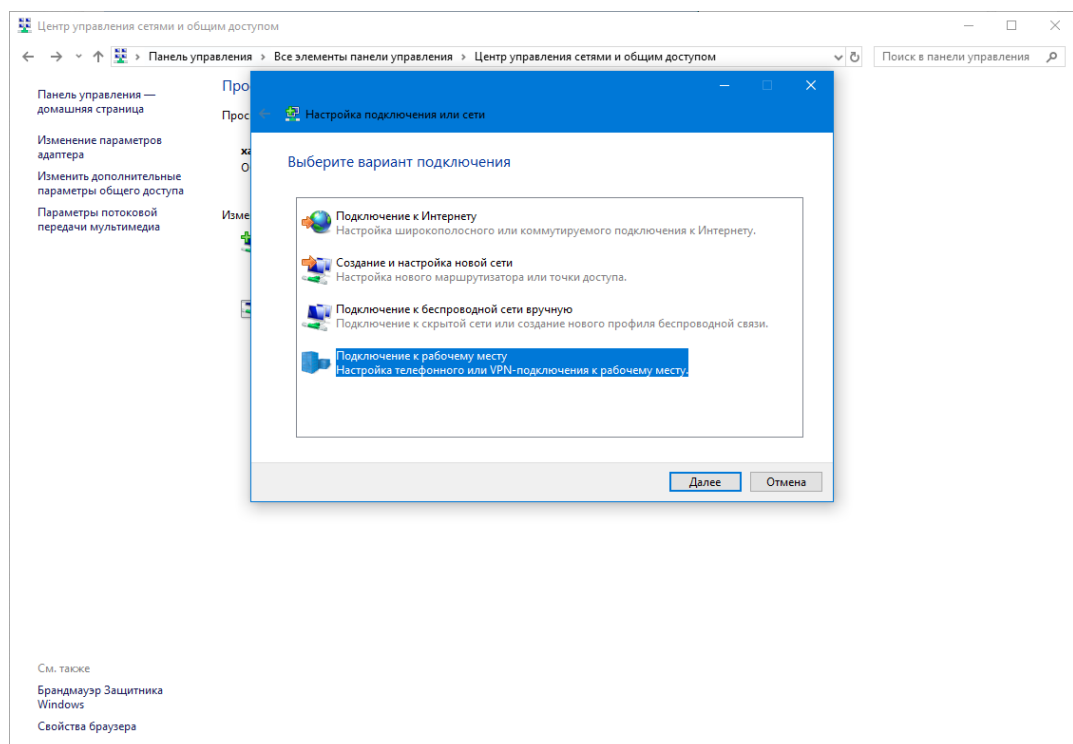
- Возможность доступа к рабочему компьютеру из дома.
- Почти полное отсутствие вероятности перехвата данных, передаваемых по VPN-туннелю.
- Если на ноутбуке установлен VPN-клиент, вы можете подключиться к своему рабочему компьютеру из любой точки мира.
- Недостатки виртуальных частных сетей
- Более сложная процедура настройки, чем предлагают менее защищенные способы. Использование VPN поддерживается оборудованием различных производителей, однако подключение к продукту, изготовленному не компанией NETGEAR, может дополнительно усложнить процедуру настройки, поскольку может отсутствовать документация, необходимая в каждом отдельном случае.
- Для подключения к сети компании может потребоваться выполнить требования политик этой компании на своем собственном компьютере.

1. Откройте "Центр управления сетями и общим доступом" (Пуск -> Панель управления -> Сеть и интернет -> Центр управления сетями и общим доступом)

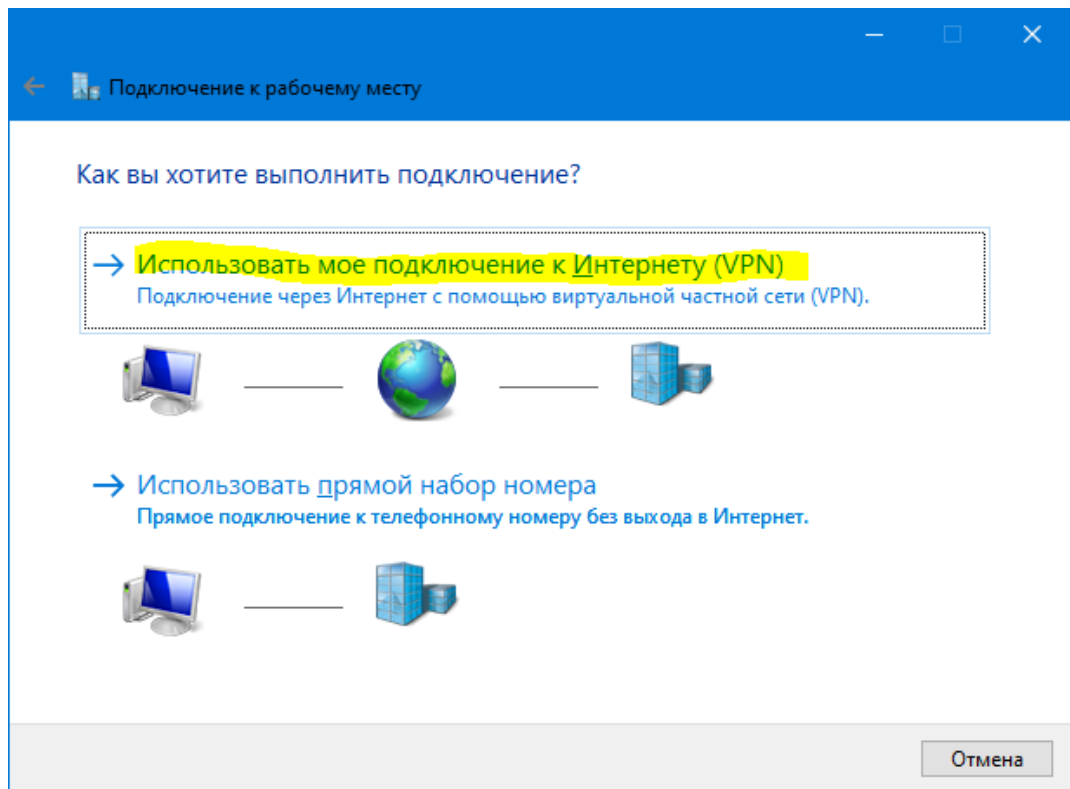
2. Во вкладке "Настройка нового подключения или сети" выберите пункт "Подключиться к сети"



3. В мастере подключения к сети выберите пункт "Подключение к рабочему месту"

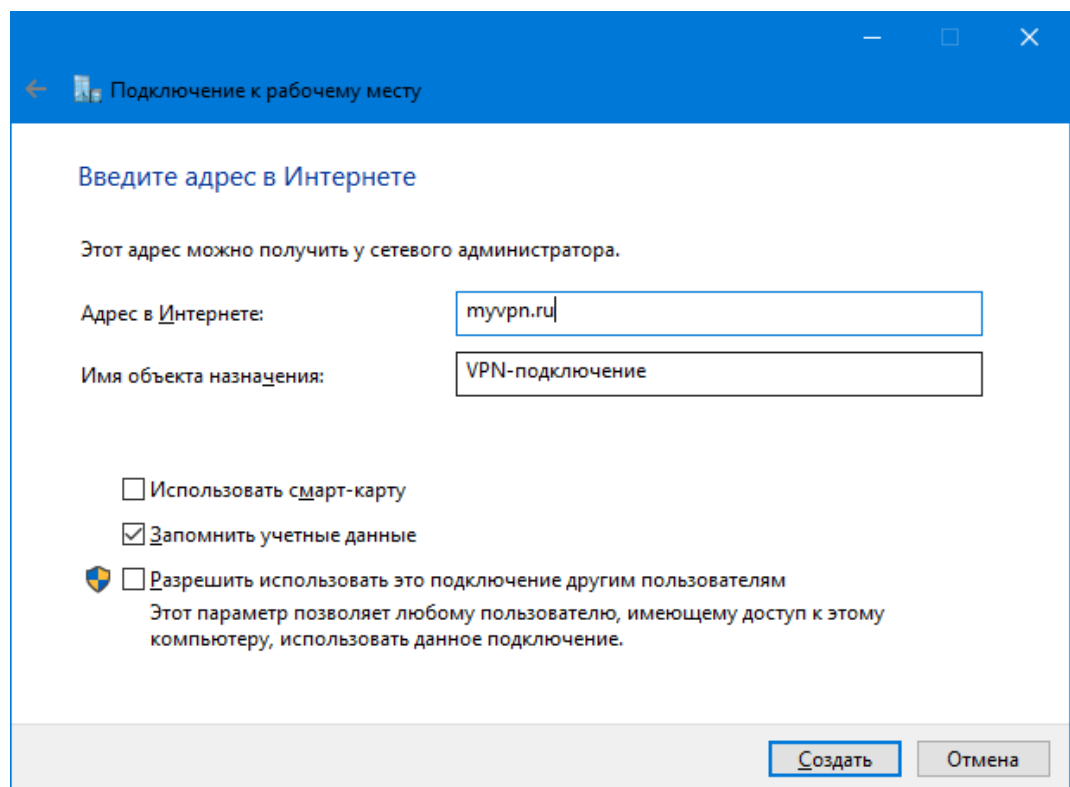


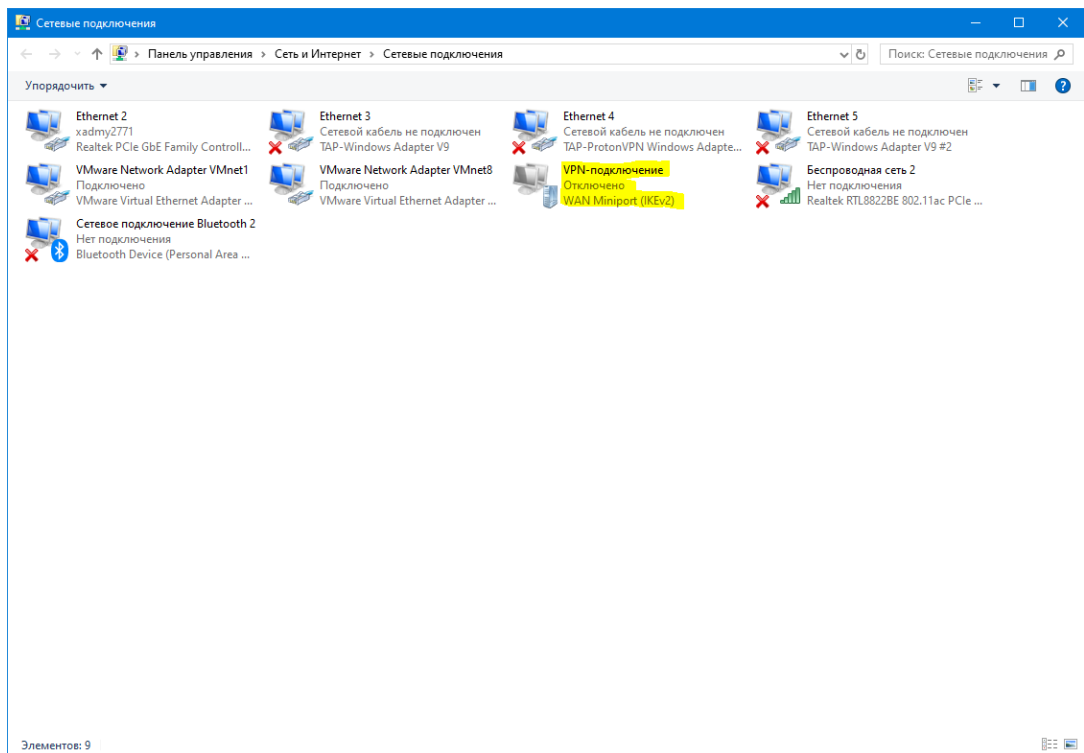
4. В мастере подключения к рабочему месту выберите пункт "Использовать мое подключение к Интернету (VPN)"



5. В появившемся окне настройки подключения к VPN введите адрес сервера и название подключения.

Подключение готово к использованию.





Практическое задание № 2.

В соответствии с вариантами задания (см. таблицу 1), используя алгоритм шифрования вручную по шагам зашифровать по шагам свою фамилию (имя, отчество). Для проверки правильности расшифровать полученный результат (при расшифровании порядок перестановок должен быть обратным). Вариант 2 метод одиночной перестановкой по ключу.

Бабич Михаил Михайлович

Таблица 1

Б	И	И	И	И	Й	В
А	Ч	Х	Л	Х	Л	И
Б	М	А	М	А	О	Ч

Ключ: Щепотка

Таблица 2

Щ	Е	П	О	Т	К	А
7	2	5	4	6	3	1
Б	И	И	И	И	Й	В
А	Ч	Х	Л	Х	Л	И
Б	М	А	М	А	О	Ч

Таблица 3

А	Е	К	О	П	Т	Щ
1	2	3	4	5	6	7
В	И	Й	И	И	И	Б
И	Ч	Л	Л	Х	Х	А
Ч	М	О	М	А	А	Б

Результат: ВЙИИИИБИЧЛЛХХАЧМОМААБ

Расшифровка

Таблица 4

Щ	Е	П	О	Т	К	А
7	2	5	4	6	3	1
В	И	Й	И	И	И	Б
И	Ч	Л	Л	Х	Х	А
Ч	М	О	М	А	А	Б

Таблица 5

А	Е	К	О	П	Т	Щ
1	2	3	4	5	6	7
Б	И	И	И	Й	И	В
А	Ч	Х	Л	Л	Х	И
Б	М	А	М	О	А	Ч

Ответ: Бабич Михаил Михайлович

Практическое задание № 3.

Вариант № 2 В сети Интернет с помощью средств поиска зайдите на сайты разработчиков и продавцов межсетевых экранов, и выполните сравнительный анализ, и выбор лучшего межсетевого экрана из трёх любых программ, используя критерий «цена и качество (безопасность)» (параметры, возможности и т.д.). Заполните таблицу результатов сравнений (пример см. таблица 1). Подготовьте обоснование Вашего выбора.

Межсетевой экран	ИКС - ПМЭ ИКС	ViPNet Personal Firewall 4	Киберсейф
Фильтрация трафика (IPv4 и IPv6)	+	+	+
Преднастроенные сетевые фильтры	+	+	+
Контроль сетевой активности приложений	+	+	-
Работа сетевых фильтров по расписанию	+	-	+
Сертифицированная версия ФСТЭК	+	+	+
Функции «Интернет Контроль Сервер» Учет трафика	+	+	+
Контроль доступа	+	+	-
Возможность развертывания программы с помощью Active Directory	+	+	
Поддержка Windows	+	+	+
Поддержка Linux	-	+	-

Дополнительные преимущества	<p>система обнаружения вторжений на основе Snort.</p> <p>Настройка провайдеров на работу с SkyDns, OpenDns и GoogleDns.</p> <p>Включение/выключение провайдеров и сетей.</p> <p>Включение в сводный отчет графиков статистики.</p> <p>Указание внешнего почтового ящика в сборщике почты.</p> <p>Настройка автоматического удаления детализированной статистики отдельно от общей статистики.</p> <p>Ведение журнала подключений пользователей с помощью Xauth.</p> <p>Добавление в мониторинг графика пинга.</p> <p>Поиск пользователей в окне импорта.</p> <p>Выключение почтовых фильтров.</p> <p>Поддержка работы с автоматически обновляемыми категориями трафика.</p> <p>Открытие доступа пользователям при редактировании VPN-сети.</p>		
Цена за пакет	28750	1300	4500
Цена на одного пользователя	2875	1300	4500

По данной сверке более выгодными и более функциональными продуктами являются ИКС - ПМЭ ИКС и ViPNet Personal Firewall 4.

Так как ИКС продается только версиями сразу на несколько устройств, то его следует брать есть количество ПК 10 и более или в случае соотрой необходимости большей функциональностью, на ПК не имеет смысла, а ViPNet Personal Firewall на 1-5 ПК.

Список используемых источников

- 1 Родичев Юрий Андреевич, «Нормативная база и стандарты в области информационной безопасности. Учебное пособие», Санкт-Петербург, «Питер»: 2017г, 256 с
- 2 Бирюков Андрей Александрович, «Информационная безопасность. Защита и нападение», Москва, «ДМК Пресс»: 2017г, 434с
- 3 Бондарев Валерий Васильевич «Введение в информационную безопасность автоматизированных систем. Учебное пособие», Москва «МГТУ им. Н. Э. Баумана», 2018г, 252с
- 4 Казарин О.В. «Безопасность программного обеспечения компьютерных систем.», Москва, МГУЛ, 2003г, 212 с.
- 5 Виктор Иванович Завгородний «Комплексная защита информации в компьютерных системах», Москва «Логос», 2003г, 260 с