https://pravo.by/document/?guid=12551&p0=HK2100091&p1=1&p5=0 – Дата доступа: 04.04.2021

4. Отчёт ЕЭК о состоянии правоприменительной практики в сфере защиты прав на объекты интеллектуальной собственности в Евразийском экономическом союзе за 2018 год [Электронный ресурс] – Режим доступа: http://www.eurasiancommission.org/ru/act/finpol/dobd/intelsobs/Documents/Отчет%20ППП%20за%202018%20год.pdf – Дата доступа: 04.04.2021

ВИРТУАЛЬНЫЕ ЧАСТНЫЕ СЕТИ (VPN), ИХ НАЗНАЧЕНИЕ И ИСПОЛЬЗОВАНИЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Липухина А.В.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

VPN – это виртуальная частная сеть, которая работает поверх сети. То есть это отдельная защищенная сеть или туннель внутри незащищенной сети Интернет. Внешне выглядит так, как если бы одна сеть была подключена к другой посредством роутера или проводов. При ее использовании осуществляется подключение к сети и обеспечивается зашифрованное соединение с нужным сервером напрямую. Провайдер может видеть подключение к какой-то одной сети и обмен данными, но какими именно – нет.

Данные остаются защищенными и недоступными для общего пользования, информацию увидят только участники VPN. Также будет невозможно идентифицировать пользователя по IP адресу и местоположению, так как будет использоваться IP адрес VPN.

Примечательно, что при таком подключении все пользователи используют единый IP адрес. Следовательно, установить, что используется подключение через VPN, несложно.

Использовать открытую и незащищенную сеть в открытых зонах Wi-Fi без VPN небезопасно, ведь в этом случае есть риск потерять пароли или конфиденциальные данные путем перехвата незащищенного трафика третьими лицами. Обычному пользователю VPN необязателен, но при ведении онлайн-бизнеса без данной сети не обойтись. Частная сеть создает зашифрованный канал, внутри которого офисы или отдельные сотрудники могут обмениваться необходимой информацией. [1] Она будет надежно защищена от несанкционированного использования посторонними. Надежность VPN трафика также заключается в том, что даже если каким-

либо образом передаваемые данные будут перехвачены, то расшифровать их будет трудно.

Сети VPN работают по следующему принципу: прокладка туннеля, шифрование данных, аутентификация. То есть, обычно защита данных происходит путем шифрования передаваемых пакетов данных либо же при помощи аутентификации обоих, отправителя и получателя, либо с проверкой на безопасность передаваемых данных или посредством создания межсетевых экранов. [2]

Несмотря на то, что VPN является хорошим средством защиты информации, такой способ работает не всегда. Например, данная сеть бессильна при внутренней атаке, если взломщик уже проник в одну из защищаемых сетей. Одной из основных проблем при работе с VPN является заметное замедление работы браузеров либо самого ПК, что объясняется тем, что поток данных проходит больше этапов, чем обычно, что может вызвать.

На сегодняшний день существует множество продуктов и инструментов ПО, которые позволяют защитить данные в Интернете от виртуальных атак злоумышленников. VPN является одним из эффективных средств защиты данных.

Литература

1. Классификация VPN-сетей// Интернет контроль сервер [Электронный ресурс]. – Режим доступа: https://xserver.a-real.ru/support/useful/klassifikatsiya-vpn-setey/. – Дата доступа: 28.03.2021.

2. Защита информации в VPN-сетях// Информационная безопасность предприятия [Электронный ресурс]. – Режим доступа: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/v-setyakh/v-vpn-setyakh/. – Дата доступа: 28.03.2021.

УДК 339.543:340

ПРАВИЛА ПЕРЕМЕЩЕНИЯ ЛИЧНОГО ИМУЩЕСТВА ФИЗИЧЕСКИМИ ЛИЦАМИ ЧЕРЕЗ ТАМОЖЕННУЮ ГРАНИЦУ РЕСПУБЛИКИ БЕЛАРУСЬ

Лукьянович Н.А.
Научный руководитель: ст. преподаватель Галай Т.А.
Белорусский национальный технических университет