ватели ввиду отсутствия глобальных экспериментов всё еще не могут прийти к единогласному мнению о безопасности использования очков виртуальной реальности. Одни считают, что вреда не больше, чем от компьютерных мониторов, другие уверены, что очки ВР ухудшают зрение, из-за аномального фокусирования изображения перед сетчаткой вследствие долгого взаимодействия с виртуальной средой.

Однако данная проблема поддаётся профилактике. Во-первых, следует выбирать качественные девайсы, многие из которых имеют регулировку межзрачкового расстояния. Во-вторых, делать перерывы на 10-15 минут каждые полчаса, и увеличивать их при малейших ощущениях дискомфорта.

Также существует правило под названием «20-20-20»: перерыв на 20 минут после 20 минут пользования ВР-гаджетом, при этом нужно смотреть на объекты на расстоянии 6 метров.

Стоит отметить, что ответственность за последствия использования ВР лежит как на производителях девайсов и разработчиках ПО (обеспечивающих взаимодействие человека с новой средой), так и на пользователях, которые в праве регулировать свое взаимодействие с новой технологией.

УДК 004.056.55

Балашкова Е.М.

## МЕТОДЫ ШИФРОВАНИЯ В МЕССЕНДЖЕРАХ

*Белорусский национальный технический университет,*
*г. Минск, Республика Беларусь*
*Научный руководитель: ст. преподаватель Липень С. Г.*

В настоящее время значительное число пользователей Интернета заинтересовано в конфиденциальности и защите личной информации. Одни заинтересованы в сокрытии сообщений от посторонних лиц, другие боятся хакеров и наблюдения со стороны государственных органов. Вне зависимости информация из переписок должна быть доступна только собеседникам, поэтому нужно уметь выбирать правильные мессенджеры.

Конфиденциальность информации обеспечивается шифрованием путем ее преобразования в нечитаемую для посторонних форму. Существует большое количество методов шифрования и появляются новые, но суть и цели всегда неизменны.

При передаче данных в сети используются два основных способа: шифрование транспортного уровня и сквозное шифрование.

Транспортное шифрование защищает информацию за счет шифрования сообщения у отправителя и передачи его на сервер, расшифровки и повторного шифрования на сервере, а также дальнейшей доставки получателю. Транспортное шифрование обеспечивает защиту информацию при передаче, однако сервер как промежуточное звено видит содержание сообщений, поэтому степень конфиденциальности зависит от отношения сервера к личной информации своих пользователей. Например, конфиденциальность сообщений будет под угрозой из-за возможных запросов правоохранительных органов или утечки данных при взломе серверов.

Использование транспортного шифрования позволяет серверу предоставлять более разнообразные услуги: хранение истории переписки, подключение к беседе дополнительных участников по альтернативным каналам (телефонный звонок в видеоконференцию), использование автоматической модерации.

Большинство специалистов в сфере информационной безопасности признают сквозное шифрование (E2EE) наиболее стойким методом защиты информации, поэтому в современных мессенджерах заявлена поддержка такого метода шифрования, но возможен и небезопасный вариант – передача данных в открытом виде без шифрования.

Сквозное шифрование представляет собой метод защиты сообщений, при котором они будут зашифрованы случайной информацией, пока не достигнут получателя. Сообщения шифруются на одном устройстве и отправляются другому человеку, при этом весь путь преодолевают в зашифрованном виде, поэтому его никто не может прочитать, кроме вашего собеседника. Это сделано для того, чтобы никто посередине не пытался подслушать сообщение, т.к. только у людей, которые принимают участие в общении, есть ключи для шифрования и расшифровки сообщений.

Следует заметить, что у E2EE свои особенности в каждом мессенджере. В мессенджере Signal реализация шифрования почти об-

разцовая, а в WhatsApp шифрование отличается лишь тем, что смена основного ключа абонента не блокирует отправку ему сообщений. В Viber сквозное шифрование можно включить самостоятельно, оно не предусмотрено по умолчанию. В Telegram E2EE применяется только в секретных чатах.

Однако, стоит оценивать значимость передаваемой информации при различных способах шифрования и защиты хранилищ данных, так как стопроцентную защиту сообщений обеспечить сложно.

УДК 37.017.92

Близнюк А.В.

## ИСПОЛЬЗОВАНИЕ ПЛАТФОРМЫ GOOGLE CLASSROOM ДЛЯ ОРГАНИЗАЦИИ УДАЛЕННОГО ОБУЧЕНИЯ

*Республиканский институт профессионального образования*
*г. Минск, Республика Беларусь*
*Научный руководитель: канд.физ.-мат.н., доцент Кравченя Э.М.*

В последнее время учреждения образования переходят на удаленную работу с использованием информационно-коммуникационных технологий. Для этого используется множество платформ. В большинстве вузов Республики Беларусь в качестве платформы для организации удаленного обучения используется система дистанционного обучения Moodle. Максимальное количество участников в Moodle составляет 20000 обучающихся, что требует создания структуры, обеспечивающей связь между ними и преподавателями. Вследствие этого вузы ищут возможности по использованию систем не требующих дополнительных расходов на ее поддержание. Одной из таких является бесплатная онлайн платформа Google Classroom. В отличии от Moodle Google Classroom не требует установки, каждый преподаватель самостоятельно создает платформу под свою дисциплину. Это упрощает организацию работы и последующий контроль учащихся. Для создания данной платформы достаточно лишь иметь аккаунт в Google. В Google Classroom можно автоматически рассылать обучающимся необходимый материал, собирать присланные на проверку работы, а также можно оставлять комментарии и замечания, получать обратную связь [1].