поближе познакомиться с различными бактериями, животными и другими объектами.

Маркетологи не упустили из виду эту технологию. При покупке недвижимости или какой-либо новой разработки, клиенту порой очень трудно понять то, что объясняет ему консультант. Для помощи, маркетологи используют ВР. Это прекрасная возможность продемонстрировать продукт со всех сторон, включая сложные технические детали и другие тонкие моменты.

Прежде всего, виртуальная реальность - это уникальная возможность окунуться в новое интересное измерение и забыть про свои ежедневные проблемы. Человек в виртуальной реальности может получить новые эмоции, а это уже неплохая профилактика стрессов.

Плюсы виртуальной реальности: проводить видеоконференции находясь в разных частях планеты; создание образовательных ресурсов/программ; создание музеев, лаборатории и других зданий; визуализация сложных объектов, физических явлений.

Каждый из нас по-своему относится к киберпространству. Для кого-то, это огромный рывок человечества и нечто новое, неизведанное и очень интересное, для других же – это повод беспокойства для своих детей.

Однако важно помнить про опасность ВР, поскольку на первый взгляд безобидные компьютерные игры могут настолько затянуть человека в свои сети, что появится зависимость, избавиться от которой будет непросто.

В целом, технология виртуальной реальности только-только начала зарождаться. Но, можно с достаточной уверенностью сказать, что научное общество ведѐт активное исследование в сторону повышения качества и более глубокого погружения пользователя в совершенно иной мир.

УДК 004.738.5

Пицко В. А., Липень С. Г.

## ФИШИНГ, КАК ВИД МОШЕННИЧЕСТВА В XXI ВЕКЕ

*БНТУ, г. Минск*

Фишинг – одна из разновидностей социальной инженерии, основанная на незнании пользователями основ сетевой безопасности и являющаяся одной из самых популярных мошеннических схем,

применяемых для получения доступа к конфиденциальной пользовательской информации.

Средства фишинг-мошенничества с каждым днем продолжают расти не только количественно, но и качественно. В то время как спам только отвлекает получателей от работы, фишинг зачастую ведет к реальным финансовым потерям.

Многие люди удивляются: а как их угораздило попасться на такой, казалось бы, очевидный обман? Дело в том, что для привлечения на ложные интернет-страницы, обычно используется почтовая рассылка или перенаправления с обычных сайтов (редирект). Для привлечения внимания в теме письма при этом указывается какая-нибудь придуманная проблема, которую якобы нужно срочно решить, перейдя по ссылке на сайт злоумышленников. А редирект используется для автоматической переадресации пользователей с нормального URL-адреса на другой, мошеннический.

Владельцы сайтов часто обнаруживают, что их веб-ресурс используется мошенниками в качестве заражѐнной фишингом площадки, перенаправляющей пользователей по совершенно другому адресу.

Технология внедрения на сайт вредоносного фишингового кода в среде профессионалов называется межсайтовым скриптингом, для обозначения которого используется английское словосочетание Cross-Site Scripting. Для термина используют сокращение «XSS», чтобы не было путаницы с каскадными таблицами стилей, использующими сокращение «CSS».

При межсайтовом скриптинге «вражеский», вирусный код устанавливается на страницы через уязвимости веб-серверов, приложений (плагинов) или же через незащищѐнные места на компьютерах конечных пользователей (это случается реже). При «взломе» сайта и установки на него вредоносного программного обеспечения содержание самих страниц иногда даже не меняется. Заходящие на хорошо знакомый им ресурс люди видят в браузере объединённый контент, который доставляется из надёжного источника. Однако, дальше происходит отлаженный мошенниками сценарий фишингового перенаправления на небезопасный сайт, копирующий оригинал, и подавляющее большинство пользователей этого не замечает.

Немалую роль в том, что многие люди становятся жертвами онлайн-мошенников, играет тот факт, что с технической точки зрения

инструменты фишинга постоянно изменяются и становятся все более и более изощренными.

Поддельные сайты уже не так легко отличить от настоящих – некоторые из них имеют вполне убедительные адреса, иногда на них даже работает защищенное соединение (HTTPS), причем с подлинными сертификатами.

В последнее время, все большее распространение приобретает мобильный фишинг – в силу технических особенностей смартфонов и планшетов распознать поддельный сайт зачастую сложнее, чем на компьютере или ноутбуке.

При этом следует иметь в виду, что в случае фишинга киберпреступнику совсем не обязательно проникать в систему устройства. Поэтому «врожденной» защиты от фишинга нет ни у одной платформы – это по-настоящему универсальная угроза.

Один из простейших способов профилактики фишинга: проверка адреса сайта в адресной строке! Если необходимо ввести свои личные данные, стоит убедится, что это именно тот сайт, на котором предварительно регистрировали учѐтную запись.

Еще одной рекомендацией является то, что на сайты, требующие ввода личных данных, переходить по ссылкам вообще не стоит – лучше набрать адрес вручную. Разумеется, посещение подобных ресурсов должно осуществляться через надежные устройства и сети.

УДК 621.762.4

Руйчева А. П.

## АВТОМАТИЗАЦИЯ ТЕСТИРОВАНИЯ ПРОГРАММНЫХ СРЕДСТВ

*БНТУ, г. Минск*

*Научный руководитель: канд. техн. наук, доцент Дробыш А. А.*

На сегодняшний день мало кто сомневается в целесообразности проведения процесса тестирования разрабатываемых программных продуктов, однако, к сожалению, не все ясно себе представляют, как тестирование грамотно внедрять и применять.

Основная задача статьи – создать достаточно чёткую картину того, что вообще из себя представляет автоматизация тестирования и когда, а также с чем её целесообразно использовать.