1. Войскунский А.Е. Психология и интернет. – М.: Акрополь, 2010. – 439 с.
2. Виртуальная реальность как метод и средство обучения [Электронный ресурс]: URL: https://cyberleninka.ru/article/n/virtualnaya-realnost-kak-metod-i-sredstvo-obucheniya (дата обращения 24.02.2019).
3. Применение виртуальной реальности в практической медицине [Электронный ресурс]: URL: https://homido.ru/news/primenenie-virtualnoy-realnosti-v-prakticheskoy-meditsine/
4. Образование и наука, VEGroup, Виртуальная реальность [Электронный ресурс]: URL: http://ve-group.ru/3dvr-resheniya/obrazovanie-i-nauka/ (дата обращения 23.02.2019).

Вредоносные программы

Шекрота И. А., Дождикова Р. Н.
Белорусский национальный технический университет

Вредоносные программы создаются специально для несанкционированного пользователем уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютеров или компьютерных сетей. К данной категории относятся вирусы и черви, троянские программы и иной инструментарий, созданный для автоматизации деятельности злоумышленников.

Необходимость создания классификации подобных объектов возникла одновременно с появлением первой антивирусной программы. Первые попытки упорядочить процесс классификации были предприняты еще в начале 90-х годов прошлого века, в рамках альянса антивирусных специалистов CARO. Но со временем от неё отказались, причиной тому стали существенные отличия в технологиях детектирования каждой антивирусной компании и, как следствие, невозможность унификации результатов проверки разными антивирусными программами. Так, классификация производителя систем защиты от вирусов “Лаборатории

Касперского" основана на разделении объектов по типу совершаемых ими на компьютере пользователей действий.

Вирусы и черви – это вредоносные программы, которые обладают способностью к несанкционированному пользователем саморазмножению в компьютерах или компьютерных сетях, при этом полученные копии также обладают этой возможностью. Классификация: Email-Worm - заражение по электронной почте, IM-Worm - программа, распространяющаяся в мессенджерах. Также одни из самых известных - Virus, передаётся по локальным ресурсам, через различные съёмные носители, а также Worm, распространяющийся через сеть. Троянские программы не способны создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения. Например, банковский троян Asacub распространяется в телефонах россиян с конца августа 2018 года. Схема заражения следующая: некий пользователь в один момент получает SMS со знакомого номера, которое содержит, например, предложение посмотреть фотографию, зайти на интересную страницу, прочитать послание от его друга. Все эти сообщения содержат неизвестную ссылку и, что более важно, имя самого пользователя, в виде обращения к нему. Откуда троян знает имя этого пользователя? Все просто: сообщения рассылаются с телефона предыдущей жертвы трояна, в них автоматически подставляются те имена, под которыми номера записаны в телефонной книге на зараженном смартфоне. Если пользователь разрешит установку приложения из неизвестного источника и запустит процесс установки, то троян запросит права администратора устройства или разрешение использовать службу специальных возможностей. Когда жертва согласится и на это, хакер далее сможет делать то, ради чего все это и затевалось (кража информации, удалённое управление устройством).

Задачей киберпреступников является внедрение вируса, червя или троянской программы в компьютер-жертву или мобильный телефон с помощью социальной инженерии и технических приёмов внедрения вредоносного кода.Методы социальной инженерии тем или иным способом заставляют пользователя запустить заражённый файл или открыть ссылку заражённого веб-сайта. Задача хакеров - привлечь внимание пользователя к заражённому файлу, заинтересовать пользователя, заставить его кликнуть по файлу (или

по ссылке на файл). «Классикой жанра» является нашумевший в мае 2000 года почтовый червь LoveLetter, до сих пор сохраняющий лидерство по масштабу нанесённого финансового ущерба. В письме было признание «I LOVE YOU», на которое среагировали очень многие, и в результате почтовые сервера больших компаний не выдержали нагрузки - червь рассылал свои копии по всем контактам из адресной книги при каждом открытии вложенного VBS-файла.

Подобные технологии используются злоумышленниками для внедрения в систему вредоносного кода скрытно. Осуществляется это через ошибки в коде или в логике работы различных программ. Современные операционные системы и приложения имеют сложную структуру и обширный функционал. Избежать ошибок при их проектировании и разработке просто невозможно. Этим и пользуются компьютерные злоумышленники. В последние годы одним из наиболее популярных способов заражения стало внедрение вредоносного кода через веб-страницы. На веб-страницу помещается заражённый файл и скрипт-программа, которая использует уязвимость в браузере. При заходе пользователя на заражённую страницу срабатывает скрипт-программа, которая закачивает заражённый файл на компьютер и запускает его там на выполнение. Для заражения большого числа компьютеров используется рассылка спама.

Спам - это электронный эквивалент бумажной рекламы, которую бросают в ваш почтовый ящик. Однако спам не просто надоедает и раздражает. Он опасен, особенно если является частью фишинга.

Спам в огромных количествах рассылается по электронной почте киберпреступниками с целью «выудить» деньги у получателей, ответивших на сообщение, чтобы обманным путем получить пароли, номера кредитных карт, банковские учетные данные и распространить вредоносный код на компьютерах получателей.

Фишинг-атаки можно назвать преступлением XXI века. Средства массовой информации ежедневно публикуют списки организаций, чьи клиенты подверглись фишинговым атакам. В то время как спам только отвлекает получателей от работы, фишинг зачастую ведет к реальным финансовым потерям. Например, летом 2014 года был обнаружен фишинг-сайт, предлагающий купить билет на чемпионат

по футболу. На самом деле вместо билета пользователь получал банковского троянца. Пробравшись в систему, злоумышленник перехватывал личные данные, прежде всего финансового характера.

Методологические и педагогические подходы совершенствования качества математической подготовки студентов технического университета

Кондратьева Н.А., Старжинский В.П.
Белорусский национальный технический университет

Для повышения уровня знаний обучающихся, формирования благоприятных условий учебного процесса, встает необходимость использования новых форм обучения, изменения существующих методов и средств, использования возможностей информационных технологий. Происходят изменения и в подходах к чтению математических дисциплин. В современном образовании актуален приоритет развития способности самостоятельно и творчески мыслить над передачей суммы знаний, умений и навыков. Но обучение действительно становится фактором развития, если оно специальным образом организовано и построено в соответствии с уровнем сформированности различных психологических функций. Это требует от педагога использования в своей деятельности теоретических представлений о развитии человека, а также современных образовательных средств, технологий, инструментов.

В математической подготовке студентовтехнического университета в настоящее время наблюдается ряд существенных проблем: недостаточная сформированность целостности математических объектов, слабая развитость логико-модельного мышления, низкая прочность знаний, умений, навыков и методов школьной математики, формализм фундаментальных знаний, неспособность их применять на практике, отсутствие у многих выпускников профессиональной мотивации и профессиональной направленности. Однако, именно математическая подготовка является одной из важных составляющих компетентности современного инженера. Общепризнано, что изучение математики способствует развитию способности к интеллектуальной и творческой деятельности, восприятию и переработке новой