6) долгий срок службы светодиодной ленты;

7) простота монтажа и эксплуатации.

«Умная» подсветка функционирует только в те моменты, когда датчики улавливают движение. Подсветка работает только в нужное время и за счет этого не потребляет много энергии и соответственно денежных средств.

Список цитируемых источников

1. *Сырокваш, А. О.* Автоматизированная система контроля доступа и учета рабочего времени на предприятии / А. О. Сырокваш, Г. М. Раковцы, А. В. Шах // Содружество наук. Барановичи-2019 : материалы XV Междунар. науч.-практ. конф. молодых исследователей, Барановичи, / М-во образования Респ. Беларусь, Барановичский гос. ун-т, Студенч. науч. о-во БарГУ ; редкол. : В. В. Климук (гл. ред.) [и др.]. — Барановичи : РИО БарГУ, 2019. — С. 87— 89 с.

2. Автоматическая подсветка лестницы своими руками [Электронный ресурс] // Лестница100. — 2021. — Режим доступа : https://zen.yandex.ru/media/id/5ab103ed20ea2b0674a31a5f/avtomaticheskaia-podsvetka-lestnicy-svoimi-rukami-5b4daa5371bf7800a9b4ba2a/. — Дата доступа : 03.04.2021.

3. *Койко, Д. Н.* Разработка подсистемы роботизированного сбора информации об уровне газов и температуры в шахте открытого акционерного общества «Беларуськалий» / Д. Н. Койко, Е. Г. Шапович // "Новатор-2020" : материалы II Баранович. науч.-образоват. форума (Барановичи, 25 сент. 2020 г.) / М-во образования Респ. Беларусь, Баранович. гос. ун-т, [ред. кол. : В. В. Климук (гл. ред.) и др.]. — Барановичи, 2020. — С. 155—160.

УДК 004.056:37

К. Е. Емжин

Учреждение образования «Белорусский государственный университет», Минск, Республика Беларусь

ПРОБЛЕМЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Введение. Развитие компьютерных технологий облегчило современный стиль жизни во множество раз. С помощью интернета люди выполняют огромное количество задач: общаются, ищут информацию, получают ответы на интересующие вопросы и просто находятся в курсе всех событий. Технологии внедряются в образовательный процесс, который становится более интересным и удобным как для преподавателей, так и для студентов. Существует достаточно большое количество университетов, использующих модель, в которой занятия проводятся в режиме онлайн. Тесты, домашние задания и исследования можно выполнять с компьютера с доступом в интернет. Благодаря интернету студентам не нужно посещать библиотеки в качестве источника для сбора информации. Различные сайты и онлайн-энциклопедии предоставляют необходимый объем знаний по любой теме, которой интересуется современный студент. В данной ситуации на одно из первых мест выдвигается такое понятие как компьютерная безопасность. Получая образование на факультете прикладной математики и информатики, не трудно заметить, насколько эта проблема актуальна для всего образовательного процесса.

Основная часть. Обратимся к источникам, которые трактуют компьютерную безопасность как совокупность технологий, процессов и методов, предназначенных для защиты сетей, устройств, программ и данных от атак, повреждений или несанкционированного доступа. В образовательной среде, где все программы и данные находятся в совместном использовании, реализация и поддержание безопасности являются необходимыми условиями защиты системы. Разумеется, что безопасность не должна мешать совместному использованию. Ее основными целями являются предотвращение неожиданной потери данных, обеспечение доступа к данным для всех уполномоченных лиц и гарантия того, что информация, хранящаяся на компьютере, никогда не будет заражена или изменена неположенным образом. Существуют наиболее распространенные и значимые формы компьютерной безопасности, такие как антивирусные программы, брандмауэры и защита паролем. Понимание данных аспектов необходимо для реализации более масштабных проектов по защите систем.

Для разработки политики безопасности требуется выделить основные типы угроз. Первые и самые распространенные — вирусы. Компьютерный вирус — это вредоносная часть компьютерного кода, предназначенная для распространения от устройства к устройству. Вредоносные самокопирующиеся программы, как правило, предназначены для повреждения устройства или кражи данных. Серьезную угрозу представляют фишинговые атаки. Студенты, преподаватели или сотрудники, которыми манипулируют для перехода по вредоносным ссылкам, могут предоставить киберпреступникам доступ к образовательной сети и ценным ресурсам. Также немало известны троянские кони, представляющие собой вредоносный код, который скрывается внутри простой программы и выполняет замаскированную функцию. Или же в качестве примера можно взять распределенную атаку типа «отказ» в обслуживании" (DDoS). DDoS — это распространенный тип кибератаки, при котором злоумышленник переполняет веб-сервер, службу или сеть трафиком, нарушающим привычный ход работы. Атаки DDoS осуществляются путем перегрузки сообщениями или запросами на

подключение целевого веб-сервера или сети. Когда целевой сервер пытается удовлетворить все запросы, он выходит за пределы своей пропускной способности и приводит к замедлению работы, аварийному завершению работы или недоступности сервера.

Имея представление об основных угрозах, необходимо выделить одни из наиболее важных шагов на пути к эффективной защите данных. Для начала стоит понимать, какие данные хранятся и в каком месте. Точно определяя свой поток данных и его уязвимые места, пользователи могут принимать обоснованные решения относительно мер, которые необходимо предпринять для защиты. Например, многие университеты используют инструменты обнаружения данных для сканирования образовательных ресурсов на предмет обнаружения конфиденциальных данных, и при обнаружении их на компьютерах, не имеющих права доступа к ним, они часто имеют возможность удалить или зашифровать их. Не мало важным является регулярное полное сканирование системы. Имея периодический график резервного копирования системы, можно будет иметь возможность восстановить данные в случае неполадок с образовательным сервером.

Большую роль в реализации надежной системы безопасности играет использование криптографии — искусства преобразования разборчивого сообщения в какую-либо непонятную форму, чтобы его содержимое не попадало в поле зрения посторонних [2]. Всё что для этого требуется — это алгоритм, который принимает дополнительный набор данных (помимо тех данных, которые должны быть обработаны), а затем корректирует информацию в зависимости от полученных значений. Этот дополнительный набор называется ключом. Ключи дают значение криптографической системе, которая идентифицирует данные, как принадлежащие конкретному пользователю, и позволяет получать зашифрованную информацию. Что касается компьютерных систем, то ключом называется просто число с заданной длиной в битах. Как объяснялось выше, ключ используется в качестве дополнительного набора данных, который учитывается в алгоритме математического шифрования для получения уникального результата для конкретного пользователя. В шифровании ключ необходим как для самого шифрования, так и для расшифровки. Зашифрованное сообщение может быть расшифровано только в том случае, если ключ, используемый для его расшифровки, соответствует ключу шифрования.

Для защиты от DDoS атак стоит использовать облачный хостинг и на это существует ряд причин. Во-первых, облако обладает гораздо большей пропускной способностью и ресурсами, чем частная сеть. С увеличением масштабов атак DDoS университетское оборудование, скорее всего, выйдет из строя. Во-вторых, природа облака означает, что оно является диффузным ресурсом. Облачные приложения могут поглощать вредоносный трафик еще до того, как он достигнет установленного места назначения. В-третьих, облачные службы управляются инженерами-программистами, чья работа заключается в мониторинге сети на предмет новейших тактик DDoS.

Создание собственной системы безопасности безусловно очень важно для образовательного процесса, ведь так шанс потери или кражи данных понижается в разы. Но помимо злонамеренных взломов существуют этические. Данные взломы включают в себя поиск слабых мест в компьютере или сетевой системе и их устранение. Наиболее распространенной формой этического взлома является тестирование на проникновение. Во время теста на проникновение, специалисты по кибербезопасности будут использовать те же методы, используемые преступным хакером в попытке сломать защиту. Если они в состоянии сделать это, они предоставят вам подробную информацию о том, как им удалось это сделать. В то время как в случае кибер-атаки у вас могут быть украдены ценные данные.

Фактические методы и процессы тестирования на проникновение будут варьироваться от уникальных потребностей. Многие университеты хотят знать, как проводить тестирование на проникновение самостоятельно, но в идеале, оно должно выполняться третьей стороной, которая специализируется на кибербезопасности. Хотя многие IT-специалисты невероятно хорошо разбираются в эксплуатации и уязвимостях в сетях, правда заключается в том, что тестировщик — это тот, кто обучен думать очень похоже на настоящего хакера, но в основе его интересов лежат интересы клиентов.

Что представляет собой тестирование? Оно начинается с поиска и выявления хостов, портов и сетевых сервисов, а затем с их идентификации. Получением данной информации занимается тестировщик на проникновение, который исследует уязвимости сети и определяет, где могут быть её слабые места. Посредством дальнейшего изучения потенциальных проблемных областей, выбирается наилучший метод создания ситуации по нарушению хода работы сети. Все это делается с учетом интересов клиентов и с конечной целью устранения любых уязвимостей.

Заключение. Таким образом, образовательный процесс станет более надежным и продуктивным при условии, если будут соблюдаться меры безопасности. Однако, всегда стоит понимать о возможных рисках. Какой бы продуманной ни была бы система защиты информации, всегда может найтись способ её взлома. Поэтому вся безопасность полагается на человека, который придерживается актуальных и правильных методов работы с компьютером.

Список цитируемых источников

1. Что такое DDoS-атака? Распределенная атака типа «отказ в обслуживании» - Cisco [Электронный ресурс] . — Режим доступа : https://www.cisco.com/c/ru_ru/products/security/what-is-a-ddos-attack.html. — Дата доступа : 19.04.2021.

2. *Шапович, Е. Г.* Системы сокрытия и шифрования информации с использованием стеганографии / Е. Г. Шапович, А. В. Шах // Сборник трудов IV Международной научно-практической конференции, 2018. — С. 101—104.