того, чтобы дерево при большой межвидовой конкуренции на своем участке смогло потребить максимально доступное количество света.

В результате анализа проведенного исследования получено, что наиболее влиятельным фактором для развития дерева в древостое является качество почвы при посадке, а свет и атмосферная влажность влияют в меньшейстепени. Полученные результаты повышают эффективность прогнозаобъема полезной биомассы, получаемой налесопосадкес момента посадки саженца, а также позволяют устранить ошибки в уходе за лесом в процессе лесовыращивания. Кроме того, полученные результаты помогают отслеживать изменения в древостое с течением времени для своевременного предотвращения чрезвычайных ситуаций и решения задач определения видового разнообразия для озеленения в лесопосадках широкого профиля.

УДК 004.93

Студ. П.А. Арцыхович
Науч. рук. доц. Н.А. Жиляк
(кафедра информационных систем и технологий, БГТУ)

ФИШИНГ. КАК ЭТО УСТРОЕНО

Фишинг – это рассылка мошеннических электронных писем и попытка обманом заставить получателей нажать на вредоносную ссылку или скачать зараженную программу, чтобы затем украсть их личную информацию. Эти письма могут выглядеть как сообщения из вполне респектабельных источников: торговых компаний, банков, а также лиц или команд в вашей собственной организации, например, из отдела кадров, от вашего руководителя или даже генерального директора. Если ваши сотрудники не могут распознать признаки фишинга, под угрозой находится вся ваша организация.

Как уже упоминалось, большинство, если не все фишинговые атаки начинаются с электронного письма, которое выглядит так, будто его отправил вполне законный источник, однако последующие способы атаки и проникновения могут быть различными. Некоторые способы достаточно просты и заключаются в том, чтобы обманом вынудить пользователя нажать на ссылку и ввести конфиденциальную информацию, другие же более изощренные, например, запуск исполняемого файла, который имитирует настоящий процесс и получает доступ к компьютеру и сети жертвы, чтобы незаметно запустить там вредоносную программу.

Вот некоторые рекомендации о том, как не стать жертвой атаки.

Лучшая защита от фишинга – знания. Злоумышленники, занимающиеся фишингом, стремятся выглядеть как можно более убедительно, но зачастую их можно раскрыть по контрольным признакам. Обязательное регулярное обучение основам информационной безопасности и социальной инженерии – это отличный способ предотвращения, который поможет вашей организации выявлять признаки вредоносных электронных писем:

- не доверяйте;
- узнайте какая информация о вас в сети;
- изучите ссылку;
- не переходите по ссылке;
- грамотно управляйте своими паролями;
- регулярное обновление ПО;
- защищайте данные.

УДК [004.056+003.26](075.8)

Студ. А.А. Иванова, К.А. Крайнов
Науч. рук. проф. Урбанович П.П
(кафедра информационных систем и технологий БГТУ)

АНАЛИЗ ЦЕЛЕСООБРАЗНОСТИ И ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ В WEB-ПРИЛОЖЕНИЯХ

Мы считаем, что недостаточно знать теорию для понимания истинного масштаба угрозы для информационных ресурсов – ведь уязвимости любого уровня, зачастую могут нести катастрофические последствия [1, 2]. Классификацией векторов атак и уязвимостей занимается сообщество OWASP. Эта организация создала список из 10-и самых опасных векторов атак на Web-приложения [3, 4]. Эти типы уязвимостей будут рассмотрены далее.

Инъекции. Все данные, хранятся в базах данных, обращения к которым строятся в виде запросов, чаще всего написанных на специальном языке запросов SQL. Злоумышленник может внедрить в форму web-интерфейса приложения специальный код, содержащий кусок SQL-запроса. Это уязвимость позволяет злоумышленнику получить доступ к данным и возможность читать/изменять/удалять информацию, которая для него не предназначена.

Недочеты системы аутентификации и хранения сессий. Для того, чтобы отличать одного пользователя от другого, web-приложение использует так называемые сессионные куки. Если ваш идентификатор украдет злоумышленник, а в системе не были реализованы проверки