Тип работы: Отчет по практике

Предмет: Информационные технологии

-

ПРИМЕНЕНИЕ СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕК-ТА
В ЗАЩИТЕ ОТ ФИШИНГОВЫХ АТАК
ВВЕДЕНИЕ
Применение защиты от фишинговых атак осложняется тем, что кибе-ратака на компьютеры в компаниях может осуществляться внезапно, когда сотрудники компании не готовы к соответствующей защите. При большом количестве атак сервера и клиентские компьютеры не выдерживают нагрузки на базы данных и сайты, следовательно возможно получение конфиденциальной информации третьими лицами, которые могут исполь-зовать полученные данные по своему усмотрению.
Сложность защиты от фишинга заключается в том, что для своевре-менного и качественного распознавания кибератаки нужно использовать большие объемы данных, быстродействующие аппаратные устройства, нанимать грамотных специалистов в сфере защиты информации, что прак-тически возможно реализовать не во всех компаниях из-за разного финан-сового состояния.
Для работы с большими объемами данных используют технологии BIGDATA, технологии машинного обучения, искусственные нейронные сети и т.д. Использование больших данных позволяет моделировать пове-дение администраторов и пользователей компьютеров при фишинговой атаке.
Когда внешнее приложение или сайт пытается получить доступ к компьютерам компании важно запретить доступ приложению или сайту за короткий промежуток времени, чтобы снизить ущерб от воздействия на компьютеры сотрудников компании. Чем больше приложений или сайтов пытается получить доступ к определенному компьютеру, тем выше веро-ятность получения доступа к конфиденциальной информации.
Использование авторизации с надежными логинами и паролями на сайтах, применение надежных паролей к учетным записям пользователей, к разным сервисам электронной почты позволяет повысить защищенность информации на уровне программного и аппаратного доступа.
Применение встроенных средств защиты операционных систем (файрволлы, антивирусные программы), программ, использующих крип-тографические алгоритмы при отправке и получении писем по электрон-ной почте позволяет повысить сложность чтения данных сторонними при-ложениями и сайтами.

СПИСОК ЛИТЕРАТУРЫ
1. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.
2. Яворски П. Ловушка для багов. Полевое руководство по веб-хакингу. – СПб.: Питер, 2020. — 272 с.
3. Масалков А.С. Особенности киберпреступлений в России: инструменты нападения и защиты информации. – М.: ДМК Пресс, 2018. – 226 с.
4. Сикорски М. Вскрытие покажет! Практический анализ вредоносного ПО. / Хониг Э. – СПб.: Питер, 2018. – 768 с.
5. Offensive Security, Тестирование на проникновение с помощью Kali Linux. – PWK 2.0, 2020. – 1033 с.
6. Колисниченко Д.Н. Секреты безопасности и анонимности в Интернете. – СПб: БХВ-Петербург, 2021 г., 256 с.
7. Дэвис Р. Искусство тестирования на проникновение в сеть / пер. с анг. В. С. Яценкова. – М.: ДМК Пресс, 2021. – 310 с.
8. Энсон С. Реагирование на компьютерные инциденты. Прикладной курс / пер. с англ. Д. А. Беликова. – М.: ДМК Пресс, 2021. – 436 с.

Эта часть работы выложена в ознакомительных целях. Если вы хотите получить работу полностью, то приобретите ее воспользовавшись формой заказа на странице с готовой работой: https://stuservis.ru/otchet-po-praktike/321490