Автор:

Орлова Анна Викторовна

студентка

Научный руководитель:

Фомичева Татьяна Леонидовна

канд. экон. наук, доцент

ФГОБУ ВО «Финансовый университет

при Правительстве Российской Федерации»

г. Москва

КИБЕРАТАКИ – ГЛОБАЛЬНАЯ ПРОБЛЕМА СОВРЕМЕННОСТИ

Аннотация*: в данной статье о кибератаках описывается тесное взаимодействие искусственного интеллекта и хакера, о самых громких хакерских атаках и о концепции их преодоления.*

Ключевые слова*: отказоустойчивое ПО, искусственный интеллект, информационная безопасность, кибератака, компьютерные системы, уязвимость.*

В современном мире параллельно стремительно развивающимся технологиям появилась тенденция к росту количества инцидентов в сфере информационной безопасности. Этот аспект приобрел особую актуальность в России. Страна заняла 2-е место по количеству кибератак, составляющих 10% от совершенных по всему миру, согласно исследованиям компании Positive Technologies (следуя за США, занявшей 1-е место (41%)). Анализируя целевую направленность злоумышленников по итогам 2017 года: получение прямой финансовой выгоды – 70%, получение различных видов информации – 26%. При этом атаки массового характера составили 57%, опережая число целевых атак. На практическом опыте были выявлены основополагающие факторы, оказывающие отрицательное влияние на информационную безопасность, а также меры по их ликвидации.

Недостаточная мотивация работника, неграмотное использование технологий или неосведомленность в сфере защиты информации может привести к утечке данных из хранилищ. Эта проблема решается методом информирования, обучения безопасному ведению работы, а также контроля усвоения информации (например: используя тестирование) с применением средств защиты почтовых серверов. Для эффективной мотивации персонала нужно использовать поощрение за правильное выполнение работы и наказание при нарушении.

Одно из самых популярных направлений атаки является использование *непроверенного кода*, уязвимость, ставшая известной еще 15 лет назад. Анализируя характер внедрений, проблема заключалась не в кодировании, а в незнании работниками проверки ввода. Необходимо кодировать отказоустойчивое ПО, тестировать его перед началом использования, вовремя устранять уязвимости. Также не следует использовать устаревшее программное обеспечение, вредоносные ссылки к непроверенным сайтам.

Пренебрежение изменением данных входа или паролей, введенных по умолчанию, стало одной из причин распределительных атак массового характера. В 1999 году пятнадцатилетний компьютерный гений Джонатан Джеймс взломал программное обеспечение NASA, с помощью которого проводилось управление Международной космической станцией. Хакерские атаки Альберто Гонсалеса, направленные на Heartland Payment System, принесли ему заработок более 10 миллионов долларов от обналичивания денежных средств с нескольких миллионов кредитных карт, а также приговор к 20 годам тюремного срока. Использование компанией одного пароля на нескольких устройствах приводит к тому, что имея доступ к одному устройству, имеешь доступ ко всем остальным. При этом отмечено, что, если защита на режимных объектах используется более трех дней, это позволяет посторонним лицам получить доступ к информации, являющейся государственной тайной. Для обеспечения максимальной защиты необходимость использования сложных паролей и их частой смены возрастает.

Неспособность распознавать несанкционированный доступ заканчивается потерей информации при работе с искусственным интеллектом. Многогранность

кибератак, использование передовых технологий, хакерских программных средств ведет к эффективной хакерской деятельности. Новый вид кибероружия в виде компьютерного червя Stuxnet был запущен в сервер ядерной программы Ирана, долгое время затормаживал работу центрифуг и выдавал неверные данные на компьютеры ученых. Противостоять таким вредоносным вторжениям становится все труднее. С целью уменьшения рисков проникновения в компьютерные системы компаний могут использоваться тщательные сегментации сетей, являющихся ключевым шагом в повышении уровня безопасности. Необходимо развивать нормативную базу в данной области с целью разработки международных актов, закрепляющих нормы ответственности за киберпреступления.

В заключение мы подходим к итогу, что информационная безопасность – «призрачное» понятие, не имеющее материального выражения. В данной статье были проанализированы современные кибератаки в основополагающих факторах, концепция их преодоления.

Список литературы

1. Крупные атаки хакеров в 2001–2016 годах: хронология [Электронный ресурс]. – Режим доступа: https://tass.ru/info/1408961

2. Джонатан Джеймс – криминальная биография хакера [Электронный ресурс]. – Режим доступа: http://www.tesla-tehnika.biz/jonathan-james.html

3. Методы защиты: решения, которые позволяют противостоять кибератакам [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/articles/metody_zashchity_resheniyakotorye_pozvolyayut