ХАКЕРСКИЕ АТАКИ

© Закиева Г.Н.[♣], Галимова В.В.[♦], Зиязтдинова Л.Н.[♥]

Нефтекамский филиал Башкирского государственного университета,
г. Нефтекамск

В статье рассматривается содержание и сущность понятия «хакер». Уделено внимание видам киберпреступников; выявлены самые известные хакеры мира. Представлены данные о киберпреступных действиях в 2015 году. Предложены меры предосторожности при работе в сети Интернет.

Ключевые слова: хакеры, хакерские атаки, киберпреступность, пользователи, страны, риск заражения, утечка данных, информация, жертвы, Интернет, персональный компьютер.

Считается, что интернет – это виртуальное отражение реальной жизни. Да, но со своими законами и поправками. Но человеческое общество одинаково, что в интернете, что вне его рамок. В человеческом обществе есть воры, жулики, мошенники и грабители. И в интернете они есть. Только красиво называются «хакерами». Термин «хакер» раньше использовался для обозначения высококвалифицированных программистов. Теперь так называют тех, кто использует уязвимости в программном обеспечении для внедрения в компьютерную систему. Часто IT-хакеров классифицируют на разные виды, из которых двумя основными являются White hat (*белая шляпа*) и Black hat (*черная шляпа*). Черными шляпами называют киберпреступников, тогда как белыми шляпами прочих специалистов по информационной безопасности (в частности специалистов, работающих в крупных IT-компаниях) или исследователей IT-систем, не нарушающих закон. В случаях, например, мелких нарушений законодательства или отсутствия нарушений законодательства, но нарушения внутренних правил какого-либо интернет-сервиса может использоваться термин Grey hat (*серая шляпа*).

[♣] Старший преподаватель кафедры Математического моделирования и информационной безопасности.
[♦] Студент кафедры Государственного управления и финансов.
[♥] Студент кафедры Государственного управления и финансов.

За всю историю существования персональных компьютеров выделилось немалое количество более известных хакеров: Кевин Митник (1983) – самый первый и самый известный хакер. Он прославился тем, что совершил одну из самых первых кибератак. Жертвой атаки была APRANet – предшественница интернета; Джонатан Джеймс (1999) – первым вскрыл систему Национального космического агентства США. Ему удалось получить доступ, взломав пароль сервера, принадлежащего другому правительственному учреждению, после этого Джеймс украл несколько важных файлов у НАСА, включая исходный код международной орбитальной станции; Leaf (2000) – этот хакер прославился тем, что выложил в свободный доступ военную систему NavstarGPS, с помощью которой задавались координаты для полетов ВВС США; Грегори Хернс (2001) – ему удалось переоборудовать один из сегментов сети NASA под хранение личных фильмов, скачанных из сети; Гарри Маккинон (2002) – ему удалось стереть некоторую секретную информацию из сети NASA и т.д. Данный перечень можно продолжать сколько угодно много, ведь с каждым годом число так называемых хакеров растет.

Далее обратимся к статистике. За 2015 год в мире было зафиксировано более 1500 утечек данных, в результате которых было скомпрометировано около миллиарда записей данных. Таковы данные отчета по индексу критичности утечек данных Breach Level Index (BLI), проведенного компанией Gemalto. Полученные результаты свидетельствуют о том, что по сравнению с 2014 годом количество утечек данных увеличилось на 49 %, а количество похищенных или скомпрометированных записей данных выросло на 78 %.

По данным индекса BLI, основной целью киберпреступников при осуществлении атак в 2015 году стали персональные данные – на долю подобных атак пришлось 54 % всех инцидентов, что больше, чем в любой другой категории, в том числе больше числа инцидентов с кражей финансовых данных. Помимо этого в 2015 году ужесточился и характер утечек данных: около двух третей из 50 наиболее серьезных инцидентов по критериям BLI произошли в 2015 году.

Что касается анализа статистики по отраслям, то в 2015 году утечки данных чаще всего происходили в розничной торговле и в секторе финансовых услуг. В розничной торговле количество утечек незначительно увели-

чилось по сравнению с прошлым годом и составило 11 % от общего количества утечек за 2015 год. В секторе финансовых услуг количество утечек данных сохранилось примерно на уровне прошлого года, однако среднее количество записей данных, скомпрометированных в результате утечек, увеличилось в десять раз – со 112 тысяч до 1,1 млн. записей.

Ситуация в сфере кибербезопасности в России, на сегодняшний момент оставляет желать лучшего. В 2015 году Россия вошла в ТОП-10 стран по числу атакованных пользователей (стоит отметить, что на долю нашей страны пришлось 251917 пользователей, подвергшихся атаке).

Таблица 1

ТОП-10 стран по числу атакованных пользователей

№	Страна	Количество атакованных пользователей
1	Бразилия	299 830
2	Российская Федерация	251 917
3	Германия	155 773
4	Индия	98 344
5	США	92 224
6	Италия	88 756
7	Великобритания	54 618
8	Вьетнам	50 040
9	Австрия	44 445
10	Алжир	33 640

Вдобавок, Российская Федерация возглавляет ТОП-20 стран, в которых отмечен наибольший риск заражения компьютеров через интернет (атакам подверглись 53,81 % пользователей). Лидер прошлого года Азербайджан опустился на третье место (49,64 %). Покинули ТОР 20 Индия, Узбекистан, Малайзия, Греция и Италия. Среди новичков – Монголия, Катар, Саудовская Аравия, Литва и Турция.

Исходя из представленных данных, можно сделать вывод о том, что Россия находится на одном из первых мест в рейтинге стран, жители которых подвержены наибольшему риску заражения и взлома компьютера через глобальную сеть Интернет.

Таблица 2

ТОП-20 стран, в которых отмечен наибольший риск заражения компьютеров через интернет

№	Страна	% пользователей
1	Россия	53,81 %
2	Казахстан	53,04 %
3	Азербайджан	49,64 %
4	Вьетнам	49,13 %
5	Армения	48,66 %
6	Украина	46,70 %
7	Монголия	45,18 %
8	Белоруссия	43,81 %
9	Молдавия	42,41 %
10	Киргизия	40,06 %
11	Германия	39,56 %
12	Алжир	39,05 %
13	Катар	38,77 %
14	Таджикистан	38,49 %
15	Грузия	37,67 %
16	Саудовская Аравия	36,01 %
17	Австрия	35,58 %
18	Литва	35,44 %
19	Шри-Ланка	35,42 %
20	Турция	35,40 %

Жертвами хакерских атак за 2015 год стали: ОАО «Банк «АВБ» (АвтоВАЗбанк), Банковская группа Citigroup Inc, интернет-аукцион eBay, сервис заметок Evernote и новостной агрегатор Feedly, Sony Pictures Entertaiment.

Для того чтобы хакерских атак стало меньше, каждый человек должен сам себя предостерегать и соблюдать элементарные меры предосторожности при работе в сети Интернет. К таковым мерам можно отнести:

1. Все больше и больше бесплатных программ (freeware) становится доступно в Интернет. Хотя это замечательное достижение является одним из самых достоинств использования открытых сетей, вы также должны быть осторожны. Некоторые из программ на самом деле могут быть опасны. Загрузка программ подвергает вас самому большому риску, так как про-

граммы могут взаимодействовать с другими компьютерами в сети, не уведомляя вас об этом.

2. Проблемы, возникающие при использовании обычной почты, также применимы и к сообщениям, передаваемым с помощью электронной почты. Например, отправитель письма может быть не тем, за кого он себя выдает. Если вы не используете специальные программы для обеспечения безопасности электронной почты, может оказаться очень трудным определение того, кто же на самом деле послал письмо. Это означает, что электронная почта не подходящий способ ведения коммерческой деятельности. Очень легко подделать сообщение электронной почты, чтобы оно казалось пришедшим от какого-то другого лица.

Другой проблемой, возникающей при использовании электронной почты, является конфиденциальность писем. Электронные письма передаются через Интернет между компьютерами. При передаче письма между компьютерами, а также при нахождении его в почтовом ящике на сервере в ожидании обращения пользователя к почтовому серверу электронное письмо доступно для прочтения другими людьми.

3. Пароли могут быть легко угаданы злоумышленником, если не принять мер предосторожности. Ваш пароль должен содержать и цифры, и знаки препинания, и заглавные и строчные буквы. Избегайте использования каких-либо слов или комбинаций слов, имен и т.д. Лучше всего использовать пароль, каждый символ которого соответствует какому-то слову. Обычно следует иметь различные пароли для различных учетных записей, но не в таком количестве, чтобы вы не смогли запомнить их. Периодически вы должны менять пароли [4].

На основании вышеизложенного, мы пришли к неутешительным выводам о том, что в век тотальной компьютеризации всех отраслей человеческой жизнедеятельности, проникновения глобальной сети Интернет во все удаленные места нашей планеты, существует большая угроза быть подвергнутым атакам, так называемых хакеров. Из года в год их число лишь возрастает. Принимаемые государством меры по борьбе с киберпреступностью не останавливают злоумышленников. Они находят все более оригинальные методы обхода барьеров.

Нужно помнить, что от хакерских атак не застрахован никто (начиная от разработчиков средств информационной безопасности и заканчивая простыми пользователями). И потому, чтобы не попасться «на удочку» «компьютерных злоумышленников», необходимо придерживаться элементарных мер предосторожности при работе с персональным компьютером и сети Интернет.

Список литературы:

1. Букин М.С. Субкультура хакеров. – М., 2008. – 672 с.

2. Макаров А.С. Теория и практика хакерских атак. – М.: Альянс-пресс, 2011. – 457 с.

3. Медведовский И.Д., Семьянов П.В., Леонов Д.Г. Атака через Интернет. – М., 2008. – 208 с.

4. Скембрей Д., Мак-Клар С. Секреты хакеров. Безопасность Microsoft Windows Server – Hacking Exposed Windows Server – М.: «Вильямс», 2007. – С. 512.

5. Скородумова О.Б. Хакеры // Знание. Понимание. Умение. – 2005. – № 4. – С. 159-161.

ПРИМЕНЕНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ В РОССИИ

© Закиева Г.Н.♣, Идиятуллина Л.Р.♦, Сафина Э.М.♥

Нефтекамский филиал Башкирского государственного университета, г. Нефтекамск

В статье рассматривается содержание и сущность понятия «электронная подпись». Уделено внимание сферам применения электронной

♣ Старший преподаватель кафедры Математического моделирования и информационной безопасности.

♦ Студент кафедры Государственного управления и финансов.

♥ Студент кафедры Государственного управления и финансов.