05.00.00 ТЕХНИЧЕСКИЕ НАУКИ

УДК 004

К. А. Василенко, Д. О. Курганов

Безопасность компьютерных сетей: от киберпреступности до шпионского программного обеспечения

Одной из основных проблем безопасности компьютерных сетей в современном мире можно назвать проблемы кибервойн, относящихся к разновидностям информационной войны. Кибервойна в дискретных сетях направлена прежде на дестабилизацию компьютерных сетей и информационных систем, а также доступа к интернету государственных учреждений, финансовых и деловых центров и создание беспорядка и хаоса в жизни стран и государств, которые полагаются на интернет в повседневной жизни.

Межгосударственные отношения и политическое противостояние часто находит продолжение в интернете в виде кибервойны и её составных частей: вандализме, пропаганде, шпионаже, непосредственных атаках на компьютерные системы и сервера, и так далее. В некоторых странах компании, которые были подвержены кибератаке, обязаны оповещать специальные госструктуры о взломе, указывая сумму ущерба. Это позволяет оценить масштаб угроз и сформировать рекомендации по защите других компаний. В нашей стране это правило касается только представителей финансового сектора.

Ущерб всей российской экономики от киберпреступников в 2018 году составил 0,25% от ВВП. Это в 2 раза больше всего российского рынка интернет-рекламы, почти половина капитализации компании «Яндекс», треть отечественного ИТ-рынка и почти половина всех расходов на здравоохранение, выделенных из бюджета РФ в 2018 году. Потери от киберпреступлений достигли 22,8% от бюджетных ассигнований на исследовательскую деятельность.

Существует два типа военных действий в киберпространстве. Их различие в целях и задачах. Первый тип — кибершпионаж, то есть несанкционированное получение информации с целью получения какого-либо превосходства, например политического или экономического. Кибершпионаж осуществляется с помощью взлома систем компьютерной безопасности и применением вредоносного программного обеспечения и различных шпионских программ, которые устанавливается на компьютер с целью сбора личной информации без согласия пользователя.

Шпионское программное обеспечение так же может изменять параметры операционной системы, устанавливать без ведома пользователя программы, перенаправлять действия пользователя, например посещение web-сайтов, что влечет за собой заражение вирусами. Изготовители шпионского программного обеспечения заявляют, что пользователи сами дают свое согласие на установку spyware. Это программное обеспечение поставляется в комплекте с дистрибутивом и указание об этом может быть указано в пользовательском соглашении, которое многие пользователи игнорируют, и, не прочитав, просто соглашаются.

Так же кибершпионаж может использоваться для защиты национальной безопасности. С недавних пор спецслужбы анализируют поведение пользователей популярных социальных сетей с целью выявления какой-либо антиправительственной или экстремистской деятельности.

Второй тип кибервойны — кибератаки. Самым старым и простым способом атак считается «MailBombing». Его суть заключается в «забрасывании» сообщениями почтовых ящиков, а иногда и целых почтовых серверов, что делает невозможным работу с ними.

Для этой цели было разработано множество различного ПО, с помощью которого даже не опытный пользователь может совершить атаку, указав только лишь e-mail жертвы. Многие такие программы делают рассылку с анонимного сервера. Такую атаку сложно предотвратить, так как провайдер может ограничить количество сообщений от одного пользователя, но с помощью программ адрес отправителя и тема генерируется случайным образом.

Усиленный интерес к материальной защищенности в комбинации с возрастающим спросом в защищенный вход к компьютерной сети заставили многочисленные государственные институты и компании стимулировать собственные старания по поиску решений, имеют все шансы увеличить защищенность концепций идентификации человека. Условия к решению имеют все шансы вносить предоставление безопасной идентификации доступа, логичного допуска (к примеру, безопасного входа в сеть) и аутентифицированного допуска к приложению, сведениям либо предложениям в организации.

По этой причине сравнительно-правовой анализ преступных деяний в области компьютерной информации по уголовному законодательству государств, которые относятся к англо-саксонской системы права, вызывает бесспорный интерес, учитывая их общий первоначальный правовой замысел, и дальнейшее индивидуальное развитие, которое базируется на своих национальных представлениях об охране информационной и компьютерной безопасности.

Впервые на законодательном уровне было введено понятие злоупотребления при помощи компьютера в Швеции в 1973 году Законом «О данных», который предусматривал введение инспекции по вычислительной технике государственных учреждений, исполняющей обязанности по контролю персональных данных, хранящихся в автоматизированных системах.

В 1977 году в США также встал вопрос обеспечения безопасности компьютерных систем и содержащейся в них информации, а также информации, которую можно было получить, используя компьютерные системы. В связи с этим был создан законопроект, который касался защиты компьютерных систем федерального уровня. Этот законопроект устанавливал уголовную ответственность за введение заведомо ложных данных в компьютерную систему; несанкционированное применение компьютерных устройств и т.п.

В Великобритании в 1984 году, под напором увеличивающейся компьютеризации и возникавших в связи с этим правонарушений в области информации, был принят Закон о защите данных, который распространял свое действие на компьютерные базы данных. Принятие этого Закона, кроме прочего, было обусловлено ратификацией Советом Европы Конвенции о защите физических лиц в отношении автоматизированной обработки данных личного характера (ETS № 108) , а также созданием благоприятных условий в конкурентной борьбе со странами Общего рынка.

Законодатели Австралии закрепили в Уголовном кодексе самостоятельный состав незаконного доступа к компьютерной информации (наряду со странами романо-германской правовой группы), в котором нет указания на родовой объект, поскольку соответствующая глава называется «Компьютерные преступления».

УК РФ, который вступил в законную силу в 1997 году, определил нормы, которые социально опасными деяниями объявляли определенные действия и конкретные бездействия в области компьютерной информации. Кроме того, они устанавливали ответственность за их осуществление. Эти нормы возникли в отечественном законодательстве впервые.

На данный момент, поскольку российское уголовное законодательство в отношении компьютерных преступлений отличается относительной «молодостью», по сравнению с УК других стран, мы имеем всего три статьи, согласно которым за совершенные преступные деяния в области компьютерной информации наступает уголовная ответственность.

Как было указано ранее, в США, Великобритании, Австралии, и особенно в Канаде, преступления в сфере компьютерной информации выделены в главу (как и в УК РФ), но могут быть как с одним только основным составом, так и предусматривать квалифицирующие признаки, к примеру, факт использования компьютерных систем может быть указан во многих статьях, и при этом дополнительная квалификация по конкретной статье не требуется.

На основании проведенного анализа можно сказать, что дифференциация преступлений в сфере компьютерной информации довольно четко прослеживается в законодательстве Канады, США и Великобритании, и меньше — в УК РФ и УК Австралии.

Если в Канаде присутствует несколько диспозиций, отмечающих преступления по различным основаниям, к примеру, распространение бесполезной информации, то в Российской Федерации мы можем увидеть только общую конструкцию преступлений, совершенных в сфере компьютерной информации, при указании квалифицирующих и особо квалифицирующих признаков, — неправомерный доступ, который повлек модификацию, блокировку или уничтожение информации; создание, использование и распространение вредоносных программ; нарушение правил эксплуатации технических средств, повлекшее модификацию, блокировку или уничтожение информации, равно как и неправомерный доступ к ней. Кроме того, недостаточно представлена и раскрыта терминология, которая не позволяет применить закон таким, какой он есть, то есть его применение порождает массу трудностей.

На самом деле, каждый государственный и корпоративный работник имеет безопасную форму идентификации. Многочисленные работодатели в наше время улучшают собственные системы идентификации, для того чтобы увеличить многофункциональные вероятности с обычный физиологической идентификации вплоть до идентификации с целью обширного диапазона дополнений, в том числе: физический допуск; подача претензий по поводу самочувствия либо иных льгот сотрудникам; надзор и руководство коллективными активами; и смена бумажный процессов онлайн-формами.

Внедрение безвредных систем идентификации людей зависит от широкого круга вопросов государственной

или корпоративной политики. В настоящее время многие системы идентификации полагаются на персонал для визуальной проверки документов с низким уровнем защиты или личности человека с фотографией, представленной для идентификации (например, паспорта, визы, водительские права), применения этих традиционных систем безопасности и процессы идентификации в повседневной жизни. Тем не менее, многие удостоверения личности с фото, включая водительские права, не используют новейшие системы безопасности идентификации или никак не применяют новые концепции защищенности идентификации либо защищенности человека и сравнительно свободно подделываются и применяются с целью аферы.

Роль смарт-карт в защищенных системах идентификации человека, широко признанных в качестве особенно безвредной и надежной конфигурацией электрической идентификации, смарт-карты имеют все шансы представлять в качестве не опасной идентификационной карты и гарантировать допуск к данным и предложениям, как через интернет, так и независимо. Благодаря потенциалу хранить, охранять и не менять данные, записанную на карту микрочипа, смарт-карта гарантирует небывалую пластичность и возможность обмена данными и передачи, обеспечивая при этом исключительную возможность получения секретных функций.

Другим видом атак является SQL-инъекция. Это атака, в ходе которой изменяются параметры SQL-запросов к БД. Запрос приобретает другой смысл и способен произвести вывод конфиденциальной информации и изменять данные.

Еще одним распространенным способом является вид атаки, называемый сниффинг, который основан на работе сетевой карты в режиме «promiscuous mode» и «monitor mode» для сетей wi-fi. В этом режиме все данные полученные сетевой картой пересылаются на обработку снифферу, то есть злоумышленник может перехватить любые данные, в любой точке маршрута данных. Если к локальной сети подключен компьютер со сниффером, то этот компьютер может получить любые пакеты со всех подключенных компьютеров.

Самым громким киберпреступлением 2016 года стал взлом почтовых ящиков Национального комитета Демократической партии США. Как сообщают СМИ, по мнению американских политиков, этот взлом повлиял на исход президентских выборов.

Методы социальной инженерии применяются злоумышленниками преимущественно вместе с вредоносным ПО (примером могут служить фишинговые сайты, содержащие ВПО), но не только. Так, в I квартале 2018 года прошла ожидаемая волна атак, нацеленных на персональные данные сотрудников американских компаний.

По данным СМИ, после введения санкций против России, увеличилось количество кибератак со стороны российских хакеров. Только за 2015 год Crowdstrike зафиксировала более 10 тысяч российских атак против компаний только одной страны. Как следствие, некоторые киберспреступники стали маскироваться под российских хакеров, имитируя русский язык в кодах.

Вредоносное ПО, которое злоумышленники использовали для атак на банки в Польше содержали большое количнство фраз на русском языке, которые якобы указывали на происхождение взломщиков. Но в действительности, оказалось, что большинство слов написано человеком, который явно не является носителем русского языка. Об этом сообщается в исследовании экспертов компании BAE Systems Сергея Шевченко и Адриана Ниша (Adrian Nish). Исследование показало, что злоумышленники использовали для перевода на русский язык Google Translate. Киберпреступники употребили несколько глаголов в неправильной форме: «установить» как «ustanavlivat» и «выйти» как «vykhodit».

Кроме того, например при разработке технологии Wi-Fi учтены некоторые вопросы информационной безопасности локальной сети, однако, как показывает практика, недостаточно. Многочисленные «дыры» в безопасности Wi-Fi дали начало отдельному течению в отрасли компьютерного взлома, так называемому вардрайвингу (wardriving — англ.). Вардрайверы — это люди, которые взламывают чужие Wi-Fi-сети из «спортивного» интереса, что, однако, не умаляет опасность взлома [1].

Несмотря на то, что в технологии Wi-Fi предусмотрены аутентификация и шифрование, эти элементы защиты работают недостаточно эффективно.

Угрозы информационной безопасности, возникающие при использовании Wi-Fi сетей, можно условно разделить на два класса:

- прямые — угрозы, возникающие при передаче информации по беспроводной связи;
- косвенные — угрозы, связанные с наличием рядом с точкой большого количества Wi-Fi- сетей.

К основным, и именно, прямым угрозам потенциально подвержен вмешательству радиоканал передачи данных. В Wi-Fi предусмотрены как аутентификация, так и шифрование, но эти элементы защиты имеют свои изъяны. Так, угроза блокирования информации в канале Wi-Fi практически оставлена без внимания при разработке технологии.

Само по себе блокирование канала не является опасным, так как обычно Wi-Fi сети являются второстепенными, однако блокирование может представлять собой лишь подготовительный этап для атаки «человек посередине», когда между клиентом и точкой доступа появляется третье устройство, которое перенаправляет трафик между ними через себя. Такое вмешательство позволяет удалять, искажать или навязывать ложную информацию.

Поисковые сервисы все чаще становятся площадкой для распространения ссылок на фишинговые ресурсы, в частности из-за возможности размещения рекламы. Так, в марте злоумышленники разместили на сайте google.com ссылку на фишинговую страницу, замаскировав ее под платное объявление, которое якобы принад-

лежало Amazon. После перехода по ссылке пользователи оказывались на сайте, имитирующем страницу поддержки Apple или Windows, где появлялось всплывающее окно, предупреждающее о том, что компьютер был заражен вредоносным ПО, а личная информация, такая как учетные данные, данные кредитных карт, была похищена. Пользователю рекомендовалось связаться со специалистами, а затем перевести им деньги, чтобы не допустить утечки украденных данных. На самом же деле это оповещение принадлежало вымогателям, которые не получали никакого доступа к данным.

Количество кибератак в мире постоянно растет. Хакеры крадут личные данные клиентов банка, пароли от социальных сетей, взламывают различные системы и сайты. Ущерб от киберпреступлений в мире за последние годы может составлять до одного триллиона долларов. Об этом сообщает «Интерфакс» в четверг, 2 февраля, со ссылкой на данные Федеральной службы безопасности (ФСБ). «Ущерб от атак хакеров по миру за последние годы составил от 300 миллиардов до одного триллиона долларов, или от 0,4 до 1,5 процента мирового ВВП», — рассказал заместитель главы профильного центра ФСБ Николай Мурашов.

Интернет не имеет границ и поэтому такие преступления зачастую имеют международный статус, то есть преступники находятся в одной стране, а жертвы в другой. Поэтому большую роль в борьбе с этим видом преступлений имеет международное сотрудничество. Таким образом, чтобы определить, как бороться с угрозами информационной безопасности в компьютерной сети и киберпреступностью, необходимо прежде всего разработать систему информирования о появлении новых киберугроз, нужно обмениваться информацией между пострадавшими компаниями, усиливать кооперацию государства и компаний.

Литература

1. Вишневский В. М., Ляхов А. И., Портной С. Л., Шахнович И. Л. Широкополосные беспроводные сети передачи информации. М.:Техносфера, 2017. 126 с.
2. Громов Ю. Ю., Драчев В. О., Иванова О. Г. Информационная безопасность и защита информации: учебное пособие. Ст. Оскол: ТНТ, 2016. 384 с.
3. Емельянов С. В. Информационные технологии и вычислительные системы. М.: Ленанд, 2016. 84 с.
4. Кияев В., Граничин О. Информатизация предприятия М.: Национальный Открытый Университет «ИНТУИТ», 2016. 235 с.
5. Мерит М., Полино Д. Безопасность беспроводных сетей / пер. с англ. А. В. Семенова. М.: Компания АйТи, ДМК Пресс, 2017. 288 с.