УДК 681.3

ИНФОРМАЦИОННОЕ ПРОТИВОДЕЙСТВИЕ В КОМПЬЮТЕРНЫХ СЕТЯХ

Голубенко А.Л., Петров А.С., Хорошко В.А.

INFORMATION OPPOSITION IN COMPUTER NETWORKS

Golubenko A., Petrov A., Khoroshko V.

В статье освещено актуальное состояние дел в области защиты информации в компьютерных сетях.

Ключевые слова: *информационная система, компьютерная сеть, интернет, защита информации.*

Информационные системы, в силу своего исторического развития, представляют собой распределенные, сложные структурные образования, которые составляют базу для управленческой инфраструктуры региона (местности, производственного комплекса); от их состояния и качества функционирования зависит не только существующий уровень экономическкого развития, но и возможности его дальнейшего роста. По сути от уровня развития информационных систем зависит экономическая самостоятельность государства.

Поэтому проблема защиты информации в современном обществе играет ключевую роль и охватила динамически социальную политическую и военную сферу деятельности людей. Причем, защита информации не является односторонней проблемой, а представляет слаженный комплекс организационных и технических мероприятий, проводимых в целях сохранения от несанкционированного доступа к интеллектуальеой собственности каждого пользователя.

Таким образом, вместе с новым тысячелетием появилось явлением информационного противодействия (ИП). Это понятие вмещает в себя процесс воздействия на компьютерную систему с использованием программно-технических средств и имеющий следствием активизацию некоторого программного средства в данной системе, приводящую к любому негативному отношению от предписанных алгоритмов работы системы. Создавшаяся ситуация обусловила разное повышение степени уязвимости информации по отношению к внутренним и внешним неконтролируемым воздействиям. Результатом таких воздействий может быть нарушение физической целостности информации (уничтожение частичное или полное или ее модификация).

В этих условиях возникает острая необходимость новых специальных мер локального, а затем и глобального характера, направленных на защиту информации. Существование глобальных компьютерных сетей еще более обостряет данную проблему. В настоящее время огромным хранилищем самой разнообразной, а главное оперативной и достоверной информации является глобальная сеть Интернет.

Популярность Интернет – в его обедоступности. Сейчас практически каждый имеющий дома компьютер и телефон, может стать ее пользователем. Однако вместе с эти многократно возрастает вероятность несанкционированного доступа к компьютеру пользователя. Помимо съема информации с помощью специальных технических устройств с телефонных линий и сети питания, теперь возможен несанкционированный съем с помощью обычной перекачки файлов по компьютерной сети.

Несомненно, что против таких вторжений существует защита. Несомненно также и то, что существует множество способов преодоления подобных защит, в результате чего возникает возможность несанкционированного доступа (похищения) очень важной, возможно секретной информации.

Основной причиной, останавливающей подобных взломщиков, является элементарность их засечки. Компьютер, через который осуществляется доступ, обязательно хотя бы на какое-то время статично привязывается к определенной географической точке. Ему необходимо осуществить связь через телефонную линию. Использование этой линии – основа практически любых компьютерных сетей. Применение и дальнейшее совершенствование мобильной телефонии позволило говорить о мобильном Интернете, т.е. об услуге доступа к сети прямо с мобильных телефонов. Мобильный телефон становится информационным термином и инструментом для электронных краж.

Таким образом, в ближайшем будущем перед нами становится проблема противодействия утечки информации через Интернет.

Внедрение технологий Bluetooth позволило связать мобильный телефон с различными электронными устройствами по радиоканалу. Это способствовало интеграции в мобильной телефоне

функции персонального компьютера. Телефон становится универсальным коммуникационным устройством. Он обладает встроенным ретроканалом для подключения электронных периферийных утройств.

По мнению экспертов взломщика уже сейчас трудно отследить, если он использует самые элементарные меры предосторожности. Взлом и несанкционированный доступ информации стал возможен из любой точки Земного шара.

Таким образом, становится ясно, что подключение компьютера, содержащего сколько-нибудь важную информацию к Интернету, равносильно выставлению всего его содержания на показ всем заинтересованным лицам. В свете такой незащищенности и прозрачности сети становится естественным вопрос об ограничении доступа в нее компьютеров, являющихся потенциальными объектами вторжения, и создании специальных закрытых корпоративных вычислительно-информационных сетей (КВИС).

Возможные каналы несанкционированного доступа к информации КВИС такие же, как и в вычислительных сетях. Единственным отличием, учитывая ее относительно малую территорию размещения, является возможность расположения каналов связи КВИС на контролируемой зоне, что значительно сокращает количество потенциальных нарушителей и в некоторых менее ответственных системах позволяет в целях экономии уменьшить прочность защиты информации в кабельных линиях связи. Для своевременного обнаружения факта несанкционированного доступа большинство КВИС используют процедуры самотестирования низкого уровня, которые должны запускаться при тестировании сети. В составе больших КВИС предусмотрены сложные системы с двойным назначением - мониторингом и диагностикой.

Можно назвать несколько каналов преднамеренного несанкционированного доступа к информации для КВИС:

доступ к КВИС со стороны штатного персонального компьютера;

доступ к КВИС со стороны кабельных линий связи питания и заземления;

доступ к КВИС при побочных электромагнитных излучениях и наводках.

Для предотвращения несанкционированного доступа к КВИС со стороны кабельных линий проводится ряд технических мероприятий противодействия с использованием активных средств (зашумление линий). Используется также способ уничтожения закладных устройств, подключенных к линиям связи с помощью специальных генераторов импульсов. Установкой специальных диэлектрических вставок в трубы систем отопления и водоснабжения, а также использованием генераторов шума можно добиться устранения побочных электромагнитных излучений и наводок опасного информационного сигнала.

Таким образом, можно обезопасить КВИС от каких-либо попыток несанкционированного проникновения и съема информации с внешней стороны. Однако вместе с тем как бы отрезается КВИС от всего окружающегго мира, лишая ее возможности свободного использования информацией, которая может быть необходима при работе. Одним из путей решения данного вопроса является использование компьюте-ра-буфера, причем как одного, так и нескольких, работа которых происходит согласно следующего алгоритма.

Компьютер-буфер находится в контролируемой зоне, и к нему применяются все те же средства защиты, которые используются на объекте. Он не является частью КВИС, однако имеет доступ в другие сети, как локальные, так и глобальные, в том числе и Интернет. Буфер не содержит в себе никакой информации и используется исключительно для скачивания необходимых данных со стороны. Причем в момент соединения с другими сетями он не имеет никаких связей с КВИС, все отни заблокированы.

После завершения сеанса компьютер-буфер отключается от внешних связей и проходит полное тестирование на предмет обнаружения в нем каких-либо вирусов, программных закладок и программ разрушителей. Следует отметить, что использование цепочки нескольких таких посредников существенно усложняет проникновение в КВИС.

Для передачи результатов, полученных в ходе научных исследований, на другую КВИС, желательно использовать обычную факсимильную и телексную связь. Причем объем информации обязательно должен быть зашифрован с помощью соответствующих криптографических программ.

На основе изложенного можно сделать вывод о реальной опасности хищения, модификации, уничтожения важной информации при использовании глобальной компьютерной сети Интернет для военно-научных и специальных целей не только в настоящем время, но и в прогнозируемом будущем. Именно невозможность дать ему адекватную оценку в настоящее время является преградой для разработки состветствующих средств информационного противодействия. Это комплексная проблема, которую можно решить только совместными усилия специалистов разных напралений – социологов, психологов, правоведови и специалистов в области защиты информации.

Что ждет сектор защиты информации в 2013 году? Проанализируем ключевые направления. Представленный ниже прогноз основывается на данных о развитии высоких технологий, состоянии киберпреступности и ситуации на рынке ИБ в прошлом году. Конечно,

мы не можем предсказать конкретных событий, но общее развитие рынков вполне укладывается в причинно-следственные связи, поэтому основные направления и способы хакерских атак вполне могут быть обозначены заранее. В статье мы постараемся проанализировать наиболее важные тенденции в трех направлениях: сами ИТ, рынок киберпреступности и средства защиты. Рассмотрим каждую из этих групп тенденций подробнее.

Общее развитие информационных технологий приводит к появлению новых удобных в использовании и экономически эффективных продуктов. Однако их разработчики не всегда могут предугадать то, как их решениями смогут воспользоваться злоумышленники. Поэтому первая группа тенденций связана с общим развитием таких технологий, как мобильные устройства, облачные вычисления и сервисы, мобильные платежи и геопозиционирование. К этой группе можно отнести четыре нижеследующие тенденции.

1.Ошибки в новых технологиях. Широкое распространение планшетных компьютеров, "мобилизация" пользователей и исчерпание ресурсов протокола IPv4 делают популярными новые технологии, которые на поверку оказываются не очень защищенными. В частности, активное использование Java в мобильных телефонах и платформах оказалась важной проблемой безопасности в 2012 году. Скорее всего, и в 2013 будут выявляться ошибки в технологиях, которые применяются в планшетах и других мобильных устройствах, — их делали в спешке, без подробного анализа проблем безопасности.

2. Переход на мобильные платформы. Мобильные платформы стали уже достаточно мощными, и хакеры начали осваивать их для проведения тех же атак, что и для персональных компьютеров. В частности, уже в 2012 году были построены зомби-сети из мобильных устройств на Android и iOS. Эта тенденция продолжится и в следующем году. Поскольку компании постепенно внедряют BYOD и все чаще позволяют сотрудникам использовать собственные гаджеты для доступа к корпоративной информации, такие устройства представляют все больший интерес для хакеров.

3. Атаки на веб-сервисы. Веб-технологии становятся все более сложным и многофункциональными. Развитие концепции AJAX в создании веб-приложений расширяет использование сценариев на языке JavaScript, в работу которых можно вмешаться со стороны. В то же время не всегда разработчики корпоративных приложений соблюдают правила безопасного создания подобных сложных систем, поэтому в большинстве из них есть достаточно серьезные проблемы с безопасностью. В 2012 году атак на эти новые приложения было достаточно много, и этот процесс не остановится и в следующем году.

4. Проблемы интеграции. Мобильные устройства и персональные компьютеры становятся все более сложными — в них начинают интегрировать модули для совершения оплаты по технологии NFC и определения местоположения по GPS. В результате и у злоумышленников появляется возможность получить доступ к функциональным возможностям этих технологий. Пока они практически не использовались "во зло", однако хакеры активно изучают их. Поэтому вполне возможно, что в 2013 году появятся новые типы атак с использованием этих модулей мобильных устройств.

Все острее проявляется проблема киберпреступности. Сегодня киберпреступники имеют достаточно финансовых ресурсов, которые могут быть вложены ими в совершенствование технологий нападения и обмана. Между злоумышленниками также существует конкуренция, которая порождает развитие технологий изготовления вредоносных программ, управления зараженными компьютерами и защитой от обнаружения. С этим связаны нижеследующие тенденции.

5. Развитие автоматизированных инструментов нападения. В отчете Sophos "Исследование угроз в сфере информационной безопасности – 2013" упомянуты проблемы, проявившиеся в 2012 году и связанные с платформами для нападения или пакетами эксплойтов, наиболее заметным из которых является Blackhole. Суть этой технологии в том, что перед совершением нападения сервер получает как можно больше сведений о программном окружении жертвы, а потом атакует ее точно подобранным эксплойтом, защиты от которого у жертвы точно нет. В 2013 году, скорее всего, развитие этих платформ продолжится и, возможно, между ними даже начнется конкурентная борьба, что может привести к созданию новых более совершенных технологий нападения.

6. Тестирование вредоносного ПО. Разработчики вредоносных программ сейчас заинтересованы в том, чтобы как можно дольше скрывать от жертвы факт взлома. Для этого нужно сделать ПО максимально незаметным для антивирусов и безошибочным. Поэтому прежде чем запускать программу, разработчикам надо протестировать ее в различных окружениях. Похоже, что в 2013 году сервисы предварительного тестирования вредоносного ПО на незаметность внедрения и работы станут достаточно популярными у разработчиков таких продуктов.

7. Захват данных. В России захват данных с помощью шифрования практикуется достаточно давно, хотя в мире эта технология начала распространяться только сейчас. Суть ее в том,

что вредоносная программа шифрует ценные данные пользователей и требует выкуп за их расшифровку. Если раньше применялись достаточно простые алгоритмы шифрования, которые позволяли декодировать данные без обращения к автору, то в 2013 году можно ожидать появления вредоносного ПО, расшифровать данные после атаки которого будет очень непросто. В частности, подобные программы стали использовать достаточно стойкие методы асимметричного шифрования и защиты своего кода от анализа.

8. Защита от антивирусов. Хакеры начали активно использовать методы запутывания исследователей антивирусных компаний, которые пытаются найти и проанализировать вредоносные коды. В частности, они постепенно применяют методы обмана репутационных фильтров и сигнатурных анализаторов. В результате вполне возможно увеличение числа ложных срабатываний этих механизмов или пропуска целенаправленных атак. Разработчики и антивирусные исследователи должны быть очень осторожны при анализе кодов вредоносных программ и поиске их в интернете. Это может привести к сокращению числа исследовательских лабораторий.

9. Хактивизм. Набирает популярность движение Анонимов за цифровую свободу, которые призывают к открытости деятельности государств и правительственных организаций. В частности, идет дискуссия о правомерности DDoS-атак как формы протеста против действий властей. Поэтому вполне возможно, что в 2013 году количество подобных атак на правительственные ресурсы только увеличится. Возможно, под удар попадут и крупные компании. Впрочем, компании, которые занимаются средствами защиты, также обладают определенными финансовыми и интеллектуальными ресурсами, поэтому разрабатывают и предлагают новые продукты, призванные помочь клиентам не потерять деньги и данные в результате атак вредоносных программ и действий хакеров. С совершенствованием защитных механизмов связаны 4 нижеследующие тенденции.

10. Модернизация операционных систем. В 2013 году ожидается замена операционных систем семейства Windows на более современную Windows 8. В ней предусмотрены новые механизмы защиты, такие как DEP, ASLR, развитие технологии песочниц и безопасной загрузки ОС. Они разработаны для блокирования уже существующих технологий нападения. Само это обстоятельство сделает новые технологии на некоторое время более безопасными — как раз в 2013 году. Дальнейшее зависит от того, насколько быстро эти механизмы защиты будут проанализированы и обойдены хакерами.

11. Многоуровневая безопасность. Как уже было сказано, разработчики вредоносных программ стремятся сделать свои продукты как можно более незаметными, поэтому создателям средств информационной безопасности не остается ничего другого, кроме как строить многоуровневые ИБ-системы, которые могли бы не только защитить от проникновения, но и обнаружить деятельность вредоносных кодов внутри предприятия. К сожалению, такие продукты более сложны в установке и эксплуатации, однако без них уже достаточно трудно говорить о полноценной защите корпоративной среды.

12. Отказ от старых технологий. Некоторые компании все еще используют сильно устаревшие вычислительные и сетевые технологии, которые уже не поддерживаются разработчиками и в них не исправляются ошибки. Поэтому защищать их становится все труднее. Бизнес стремится отказаться от них и перейти на решения, более совершенные как технологически, так и по уровню защищенности. В частности, одним из таких направлений модернизации является протокол IPv6, который имеет встроенные механизмы шифрования и контроля целостности. Некоторые компании стремятся перейти с устаревших уже мейнфреймов на более современные системы на базе Linux. Защиту современных систем можно сделать достаточно надежной и контролируемой.

13. Защита Больших данных. Одной из важных тем 2012 года было появление систем для обработки больших массивов данных. Их уже начали создавать, и возникла задача обеспечения безопасности. Принципиальных проблем для создания инструментов защиты Больших данных нет, поэтому в 2013 году они, скорее всего, появятся на рынке и будут активно предлагаться разработчиками.

Мы перечислили лишь основные тенденции 2013 года, которые характерны и для рынка IT. Есть и другие факторы развития, связанные исключительно с локальными особенностями: черным списком запрещенных сайтов, распространением технологии электронной подписи и выдачей универсальной электронной карты (УЭК). Они также дополняют перечисленные тенденции в части новых технологий и средств защиты.

Литература

1. ISO/IEC 15408:1999(E) Information technology – Security techniques – Evaluation criteria for IT security, First edition, 1999-12-01.

2. Трубачев А.П., Долинин М.Ю. и др. Оценка безопасности информационных технологий. Серия «Безопасность информационных технологий». – М.: СИП РИА, 2001. – 356 с.

3. Сидак А.А. Формирование требований безопасности современных сетевых информационных технологий. Серия

«Безопасность информационных технологий». – М.: МГУЛ, 2001. – 278 с.

4. Общие критерии оценки безопасности информационных технологий: Учебное пособие. Перевод с английского Е.А. Сидак/Под ред.. М.Т. Кобзаря, А.А. Сидака. – М.: ЦБИ, 2001. 81 с.

R e f e r e n c e s

1. ISO/IEC 15408:1999(E) Information technology – Security techniques – Evaluation criteria for IT security, First edition, 1999-12-01.

2. Trubachev A.P., Dolinin M. and others. Assessment of safety of information technologies. A series of «Security of information technologies». - M: SIP RIA, 2001. - 356 p.

3. Sydak A.A. The formation of the security requirements of modern information technology network. A series of «Security of information technologies». - M: MSFU, 2001. - 278 p.

4. General Criteria security evaluation of information technology: Textbook. Translated with English E.A. Sydak / Ed. M.T. Bard, A. Sydaka. - Moscow: TSBY, 2001. 81 p.

Голубенко О.Л., Петров О.С., Хорошко В.О.

ІНФОРМАЦІЙНА ПРОТИДІЯ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

У статті висвітлений актуальний стан справ в області захисту інформації в комп'ютерних мережах.

Ключові слова: *інформаційна система, комп'ютерна мережа, інтернет, захист інформації.*

Golubenko A., Petrov A., Khoroshko V.

INFORMATION OPPOSITION IN COMPUTER NETWORKS

In the article the actual state of businesses is lighted up in area of priv in computer networks

Keywords: *informative system, computer network, internet, information protection.*

Голубенко А.Л. – Герой Украины, д.т.н., проф., чл.-корр. АПН Украины, ректор ВНУ им. Владимира Даля.

Петров Олександр Степанович – докт. техн. наук, професор, завідувач кафедри безпеки інформаційних систем, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.

Хорошко В.А. – д.т.н., профессор кафедры «Безопасность информационных технологий» Национального авиационного университета (г. Киев).

Рецензент: Ульшин Віталій Олександрович – докт. техн. наук, професор, професор системної інженерії, Східноукраїнський національний університет імені Володимира Даля, м. Луганськ.