УДК 004.056.53

С.А. Петренко

МОДЕЛЬ КИБЕРУГРОЗ ПО АНАЛИТИКЕ ИННОВАЦИЙ DARPA

Петренко С.А. **Модель киберугроз по аналитике инноваций DARPA.**
Аннотация. В работе рассматривается задача определения актуальной модели киберугроз цифровой обработки данных по аналитике инноваций DARPA. С 2002 года агенство DARPA проводит широкий спектр научных исследований для достижения и сохранения технологического превосходства вооруженных сил США в киберпространстве. В соответствии с этим задача определения актуальной модели киберугроз цифровой обработки данных рассматривается как адаптивная коррекция современных киберугроз по текущим НИОКР DARPA.
Ключевые слова: научные исследования, объект информатизации, киберугрозы, модель киберугроз, инновации, кибербезопасность..

Petrenko S.A. **Model Cyber Threats by Analysis of DARPA Innovations.**
Abstract. This paper considers the problem of determining the actual model cyber digital data analytics innovation DARPA. Since 2002 DARPA agency conducts a wide range of research to achieve and maintain the technological superiority of the US military in cyberspace. According to this research, the problem of determining the actual cyber digital data processing is regarded as adaptive correction of modern cyber threats on current R&D DARPA.
Keywords: research, cybersecurity, cyber threat, cyber model, innovation, the object information.

1. Введение. В настоящее время ряд технологически развитых государств (более 20 стран) продекларировали разработку «кибероружия». В США в декабре 2011 года от Конгресса было получено разрешение на развитие «наступательного» кибероружия. Во Франции в 2008 году в «Белой книге по обороне и национальной безопасности» введено понятие «кибервойна» и раскрыты ее составляющие – «кибероборона» и «наступательные возможности для кибервойны». В Германии в феврале 2011 года принята «Стратегия безопасности в киберпространстве». Аналогичный документ введен в действие в Великобритании с ноября 2011 года.

Для разработки «кибероружия» упомянутыми странами проводится широкий спектр НИОКР. В частности, в США ведутся работы по созданию специальных программно-аппаратных комплексов: *«PRISM» (сбор и обработка метаданных), «Feed through», «Gourmet through» и «Jet p low» (дистанционное внедрение «закладок» в персональные компьютеры), «Quantum Insert » (перенаправление трафика к ложным сайтам Интернета), «Dropout Jeep» (дистанционный съем информации с айфонов фирмы «Apple»), «Monkey calendar» (sms-сообщения о местонахождении мобильных телефонов), «Rage master» (перехват информации с экранов компьютеров), «Genie»*

(контроль функционирования 85000 «закладок-шпионов» по всему миру). На примере инноваций DARPA покажем возможные современные направления поисковых исследований в области кибербезопасности и определим модель новых киберугроз.

2. Проекты DARPA. Катастрофические последствия 11 сентября продемонстрировали неспособность США к отражению подобных терактов, беспрецедентных как по своему масштабу, так и асимметричности вызовов безопасности. Для разрешения сложившейся ситуации DARPA инициировала ряд специальных НИОКР [1–3] с бюджетом финансирования от 500 млн (2002-2005 годы) до 1 млрд долл. (2002-2009 годы). Проект «Предупреждение террористических актов» (Terrorism Information Awareness - TIA) позволил на основе анализа большого количества разнородных данных о слабо связанных между собой событий, таких как покупка авиа- и железнодорожных билетов, бронирование номеров в гостиницах, покупка химикатов и взрывчатых веществ, приобретение огнестрельного оружия и др., выявлять преступные группы лиц, готовящихся совершить террористический акт с применением оружия массового уничтожения (ядерного, химического, биологического) на территории США. Для реализации проекта были привлечены модели и методы системного анализа, исследования операций, теории игр, теории вероятности и статистического анализа, теории принятия решений и пр. Другой проект DARPA был направлен на разработку специализированного программного обеспечения так называемого "ситуационного анализа" (Software for Situational Analysis), который позволил в автоматизированном режиме: распознавать людей на расстоянии, обнаруживать противника, осуществляющего наблюдение за целями (объектами критической инфраструктуры) на территории США; автоматически находить, извлекать и связывать между собой отрывочные и фрагментарные представления о намерениях и деятельности групп людей, содержащиеся в больших массивах открытых и закрытых источников информации; достаточно точно моделировать субъективные представления и социальное поведение малочисленных по составу групп для имитации и проигрывания асимметричных действий противника; обеспечивать более эффективные средства анализа и принятия решения для пресечения преступной деятельности. Проект «Моделирование асимметричных воздействий» (Wargaming the Asymmetric Environment - WAE) позволил выявлять мотивы и своевременно раскрывать замысел террористических действий. В результате были созданы имитационные модели поведения отдельных людей и небольших групп с учетом их психологии, культуры, политических взглядов, уровня образования и жизненного

опыта (Scalable Social Network Analysis - SSNA). Также были разработаны имитационные модели поведения отдельных враждебно настроенных стран, их ключевых политических лидеров и террористических групп. Кроме того, построены аналитические модели для принятия решений, позволяющие прогнозировать различные ситуации в реальном масштабе времени (Rapid Analytical War Gaming - RAW). Здесь был применен математический аппарат теории игр со смешанными стратегиями, а также теория принятия решений в условиях неопределенности. Для повышения эффективности и координации совместных действий американских спецслужб по своевременному обнаружению террористов, раскрытию их замыслов и предотвращению терактов DARPA инициировала проекты «Генуя» и «Генуя-2». В результате была создана так называемая "динамическая виртуальная среда" для снятия возможных организационных и технических барьеров в совместной работе специалистов различных ведомств и организаций. В основу были положены модели и методы нечеткого структурирования аргументов, трехмерной цветной визуализации и организации адаптивной памяти.

Для обеспечения устойчивости и живучести критически важных объектов государственного и военного управления в чрезвычайных условиях DARPA инициировала долгосрочную программу – «Научные и инженерные методы» (Information Assurance Science and Engineering Tools - IASET), - которая объединила усилия специалистов в смежных областях знаний (исследование операций, системотехника, вычислительные системы и сети, кибербезопасность, операционные системы, базы данных и др.).

Проект «Безопасные и живучие информационные системы» (Organically Assured and Survivable Information Systems - OASIS) позволил выработать новые архитектурные решения комплексной системы защиты критических важных информационных систем. В результате была создана новая клиент-серверная технология обеспечения устойчивости и живучести вычислительных систем на основе современных методов обнаружения вторжений, адаптивной защиты, отказоустойчивости и реконфигурации.

Для оперативного контроля и прогнозирования состояния критически важных информационных систем реализован проект «Новые методы обнаружения кибератак» (Advanced Network Surveillance), в рамках которого созданы новые технологии обнаружения массовых и групповых кибератак. Создан прототип самообучающейся системы контроля и прогнозирования состояния критически важных информационных систем в условиях воздействия противника.

В рамках проекта «Корреляционный анализ кибернападения» (Cyber Attack Data Correlation) были разработаны адаптивные методы корреляционной обработки и классификации регистрируемых данных о состоянии критически важных информационных систем в условиях массовых враждебных программно-математических воздействий. Основное назначение – использование в крупных территориально-распределенных вычислительных сетях для определения фактов скоординированного широкомасштабного кибернападения и последующего адекватного противодействия.

В 2014 году на сайте DARPA (www.darpa.mil/Our_Work/I2O/Programs) был опубликован актуальный перечень поисковых программ исследований [3], в том числе:

- Профилирование поведения пользователей (Active Authentication);
- Активная киберзащита с ложными целями (ACD);
- Обнаружение аномальных процессов в обществе (ADAMS);
- Автоматизированный анализ кибербезопасности (APAC);
- Инфракрасный страж (ARGUS-IR);
- Высоконадежный семантический транслятор (BOLT);
- Адаптивная система (CRASH);
- Поисковая компьютерная система (CSSG);
- Формальная верификация (CSFV);
- Противодействие инсайдерам (CINDER);
- Глубокая очистка контента (DEFT);
- Психофизическая защита (DCAPS);
- Высоконадежная киберзащита беспилотных летательных аппаратов (HACMS);
- Семантический анализ (ICAS);
- Поиск контента (Memex);
- Повышение устойчивости программного обеспечения (MUSE);
- Транспарентные вычисления (Transparent Computing);
- Создание «живучего облака» (MRC);
- Рубрикация и семантическая классификация документов (MADCAT);
- Боевые операции в киберпространстве (Plan X);
- Надежное программирование (PPAML);
- Криптозащита вычислений ((PROCEED);
- Автоматизированный перевод речи (RATS);
- Безопасные коммуникации (SAFER);

- Работа в социальных СМИ (SMISC);
- Программа контроля НДВ в закупаемом для нужд Минобороны США ПО (VET);
- Наглядная визуализация (VMR);
- Распознавание сетей (WAND);
- Большие данные (XDATA) и пр.

Например, *программа MUSE* предназначена для повышения надежности и безопасности прикладного программного обеспечения на основе методов надежности программ, машинного обучения и формальной верификации программного обеспечения.

Другая программа «Автоматизированный анализ кибербезопасности мобильных приложений» (*Automated Program Analysis for Cybersecurity - APAC)* позволяет осуществлять контроль не декларируемых возможностей (НДВ) в мобильных приложениях в автоматизированном режиме.

Программа (*Integrated Cyber Analysis System - ICAS)* посвящена разработке новых методов автоматического обнаружения и нейтрализации кибератак на основе интеллектуального анализа данных и выявления скрытых закономерностей.

Программа *(Safer Warfighter Computing - SAFER)* предусматривает создание программных средств компьютерной разведки и преодоления средств защиты информации противоборствующей стороны.

В рамках программы Supply Chain Hardware Intercepts for Electronics Defense предполагается разработать миниатюрный (100X100 мкм) и недорогой (меньше одного цента за штуку) чип, который будет подтверждать аутентичность электронных компонентов. Чип будет находиться внутри корпуса микросхемы, но никак не будет электрически связан с ее функциональной начинкой и не должен требовать существенных изменений процесса производства. Ожидается, что эта разработка будет иметь большой успех и на рынке потребительской электроники, где производители не всегда способны проконтролировать качество всех необходимых компонентов (учитывая огромные темпы развития полулегального китайского фабричного производства).

Программа (*Crowd Sourced Formal Verification - CSFV*) направлена на решение сложных аналитических задач в игровой форме. Сложные математические задачи можно представить в виде интересных и увлекательных онлайн-игр.

Программа-конкурс (*Cyber Grand Challenge - CGC*) направлена на разработку приложений для автоматического исправления уязвимостей так называемого нулевого дня, 0-day, в том числе для тестирова-

ния программного обеспечения, выявления уязвимостей, генерации патчей и установки их в компьютерной сети. Сегодня поиск уязвимостей и так частично автоматизирован. Есть методы статичного и динамичного анализа, которые способны обнаружить характерные уязвимости в коде. Но вот исправлять эти ошибки автоматически компьютеры пока не научились. Задача программы - совместить анализ кода и защиту сетей в единый программно-аппаратный комплекс. Задача чрезвычайно сложная, но и 2 миллиона — достойная награда за победу в названной программе-конкурсе. Заметим, что название Cyber Grand Challenge связано с известным конкурсом Grand Challenge, который трижды проводился для автономных транспортных средств в 2004-2007 гг. Десятки автомобилей-роботов пытались проехать по незнакомой пересеченной местности, прокладывая маршрут и объезжая препятствия, включая канавы, камни и узкие тоннели. Маршрут объявляли за два часа до начала конкурса. Если в первый год проведения DARPA Grand Challenge ни одна машина не доехала до финиша (собственно, только 8 из 15 машин смогли уйти со старта, а лучшая команда преодолела 11,8 км из 230), то потом они уже начали соревноваться на скорость. Прогресс был очевиден. По аналогии и с Cyber Grand Challenge — поначалу задача кажется неразрешимой, но в дальнейшем ожидается получить первые самообучающиеся прототипы, которые действительно смогут автоматически генерировать патчи и закрывать уязвимости нулевого дня, 0-day, в течение нескольких секунд после обнаружения. Конкурс Cyber Grand Challenge пройдет в несколько этапов и будет продолжаться несколько лет. В ближайшее время опубликуют информацию о грантах на разработку технологий для проведения этого конкурса, в том числе на создание набора задач. Финал соревнований состоится в первой половине 2016 года.

Программа *Gargoyle* направлена на создание систем киберзащиты, работающих на скоростях более 10 ТБ/сек. Развитие вычислительных возможностей телекоммуникационных средств существенно запаздывает, не справляясь со все возрастающим потоком данных. Результат – пропущенные предупреждения и запоздалая реакция. Например, совокупный мировой поток данных через оптоволоконные кабели в настоящее время составляет более 100 ТБ/сек и, как ожидают, превысит 1 ПБ/sec к 2020 году. В рамках программы Gargoyle в DARPA разрабатывают фотонные корреляторы для обработки критически значимой информации, которые обеспечат почти нулевое время ожидания данных. Для этого создадут широкополосную модуляцию с прямым расширением спектра полосы пропускания более 10 ГГц.

Программа *"Разработки нового беспроводного стандарта связи" (100 Gb/s RF Backbone).* Сейчас в армии США для различного рода коммуникаций применяется безопасный беспроводной протокол Common Data Link (CDL). Он обеспечивает максимальную скорость передачи данных на уровне 250 Мб/с. Однако этой скорости уже недостаточно для полноценного управления беспилотными летательными аппаратами, отправления и получения разведывательных данных. Цель программы 100 Gb/s RF Backbone – создание нового беспроводного стандарта связи, который способен обеспечить скорость передачи данных 100 Гб/с при радиусе покрытия 200 км. При этом требования к массе конечного оборудования и уровню его энергопотребления предъявляются такие же, как и к оборудованию CDL.

В рамках программы *"Разработки новой навигационной системы на смену GPS" (Adaptable Navigation Systems)* разрабатывается система, которая позволит военнослужащему ориентироваться в любых условиях, в том числе тогда, когда сигнал GPS недоступен (например, в результате радиоэлектронного противодействия, особенностей ландшафта и природных явлений). Предполагается, что, во-первых, будет разработан инерциальный измерительный блок нового типа, которому требуется меньше фиксаций координат от системы GPS, например, за счет использования сверхкомпактных атомных часов, работающих с холодными атомами. Во-вторых, будет создан метод использования эфирных сигналов (SoOp) от различных источников – наземного, воздушного и космического базирования. В-третьих, будет улучшена навигация по геофизическим полям. В результате должна появиться новая многоцелевая навигационная система, которая сможет изменять конфигурацию в полевых условиях для работы произвольного оборудования в различных условиях эксплуатации.

Программа *XDATA* направлена на создание систем киберзащиты на основе больших данных, Big Data. В рамках упомянутой программы в открытом каталоге *DARPA* представлены проекты с исходными кодами на *GitHub* под свободными лицензиями: *ALv2, BSD, GPL, GPLv3, LGPL, MIT и др. В* том числе, библиотека на языке Python компании *Continuum Analytics* для интерактивной визуализации «больших данных»; *Bokeh д*ля «тонких» клиентов; библиотека для построения масштабируемых байесовых сетей *SMILE-WIDE* для Boeing с соответствующим API-интерфейсом (представляет собой аналог известного API SMILE, который дополнительно способен исполнять векторные операции за счет распределенной реализации на Hadoop), оптимизирующий компилятор Numba для Python, разработанный Continuum Analytics, Inc. под лицензией BSD и пр.

3. Модель киберугроз. Анализ результатов поисковых исследований агенства DARPA в области кибербезопасности, а также ряда смежных НИОКР свидетельствует о появлении и необходимости нейтрализации новых классов угроз кибербезопасности [4–10]. В том числе, следующих киберугроз цифровой обработки данных:

Угроза подключения к каналам связи.

Цифровая обработка сигналов дает возможность копирования («ответвления») голосового трафика в пределах коммутационной матрицы без каких бы то ни было демаскирующих признаков. Факт копирования невозможно отследить, он не вызывает ни изменений в амплитуде передаваемого сигнала, ни искажений, связанных с задержкой передачи. Это является качественным отличием современных вычислительных систем и сетей.

В частности, практически все крупные разработчики оборудования реализовали в программном обеспечении те или иные возможности копирования речевого трафика при наличии у прослушивающей стороны соответствующих полномочий, определенных администратором. В некоторых случаях это полноценная трехсторонняя конференцсвязь с отключенным входящим голосовым каналом от прослушивающей стороны, в других – ответвление потока по специальной схеме при наборе определенного номера. Некоторые исследователи в области информационной безопасности отдельно выделяют так называемый «полицейский режим» – возможность выполнения тех же операций извне, при наборе из городской телефонной сети определенного номера, принадлежащего номерному полю УАТС, и кода допуска

Цифровые учрежденческие АТС модели AVAYA Definity реализуют возможность скрытого копирования речевой информации в рамках возможности «Service Observing» (Контроль вызова), позиционируемой как средство для контроля со стороны менеджеров за ходом работы телефонных операторов, в первую очередь в Центрах обработки вызовов. Активация функции возможна как в варианте с подачей в речевой канал предупредительного сигнала каждые 12 секунд о факте прослушивания третьей стороной, так и без него. Настройка полномочий на прослушивание выполняется с консоли администратора по групповому принципу: каждой абонентской линии соотносится класс приоритетов «COR», а в матричной форме для каждой пары классов определяется разрешение или запрет прослушивания. Активация прослушивания выполняется набором кода доступа к сервису, а затем номера абонента, и может быть назначена на одну из функциональных клавиш прослушивающего аппарата. Кроме того, при определенной

настройке возможен доступ к функции с внешних линий, например, с городской телефонной сети.

Сервер IP-телефонии CallManager от компании Cisco Systems Inc. также предоставляет возможность включения в разговор третьего абонента, обладающего достаточными полномочиями (как с предупредительным сигналом, так и без него). Функция именуется «Barge In» и имеет две различные схемы технической реализации.

1) Схема на основе программно-аппаратных средств, штатно встроенных во все IP-аппараты компании с 2-мя линиями. Прослушиваемый IP-аппарат при поступлении запроса на конференц-связь (в т.ч. одностороннюю – прослушивание) самостоятельно выполняет ответвление и микширование двух голосовых потоков (первичного – в направлении абонента и вторичного – в направлении прослушивающего устройства) аппаратными средствами второй линии. При этом при соответствующей настройке предупредительных сигналов в первичный голосовой поток не добавляется, более того, на дисплее прослушиваемого IP-аппарата не появляется никаких информационных признаков о факте подключения. Данная схема ограничена только одним подключением прослушивания и только широкополосным (64 кбит/с) кодеком G.711, однако, не вносит никаких демаскирующих искажений в голосовой поток.

2) Схема на основе выделенных программно-аппаратных средств конференц-связи сервера IP-телефонии. При поступлении запроса сервер IP-телефонии замыкает голосовой трафик в обоих направлениях (проходивший до этого момента напрямую между IP-устройствами) на устройство конференц-связи и с его помощью выполняет микширование и ответвление данных (в этом случае уже на неограниченное количество прослушивающих устройств и вне зависимости от используемого абонентами кодека). Недостатком схемы по сравнению с первым вариантом является слышимое искажение («провал голоса») в момент переключения потоков.

Настройка привилегий на прослушивание выполняется отдельно для каждой прослушиваемой линии (непосредственно указывается набор линий, имеющих право на подключение, в т.ч. незаметное, к разговору).

Таким образом, получение противником тем или иным образом привилегий администратора предоставляет ему практически неограниченные возможности по незаметному прослушиванию.

Угроза прослушивания разговоров в помещении с помощью автоответа.

Цифровые и IP- аппараты, как сложные компьютерные устройства, привнесли еще один класс угроз утечки речевой информации, связанный с возможностью удаленного (в т.ч. при некоторых условиях – несанкционированного) включения микрофона и передачи разговоров, ведущихся в помещении по цифровому каналу. В качестве первого, рассмотрим вариант, не связанный с недокументированными возможностями самих аппаратов – широко распространенную опцию «Автоответ». При ее активации вызываемый аппарат при поступлении вызова подает один (часто – укороченный) сигнал вызова, а затем автоматически включает микрофон и громкоговоритель с тем, чтобы абоненты имели возможность общаться между собой по громкой связи либо с использованием гарнитуры.

При возможности настройки опции «Автоответ» в зависимости от вызывающей линии (интерком) она начинает представлять реальную угрозу прослушивания разговоров, ведущихся в помещении. Злоумышленник, получивший привилегии администрирования УАТС, может создать интерком-группу, включив в нее атакуемую линию и свой номер, изменить сигнал вызова со своей линии на запись тишины и получить тем самым возможность прослушивать разговоры в помещении, сделав вызов на данную линию. Схема обладает некоторыми незначительными демаскирующими признаками: 1) в зависимости от модели аппарата факт включения микрофона может отражаться индикаторами, 2) линия в момент прослушивания будет занята при попытке вызова извне, и 3) существует риск поднятия прослушиваемым абонентом трубки для выполнения вызова. Однако, это не исключает возможность выполнения успешного и скрытного прослушивания, особенно в ситуациях, когда в помещении идет активное обсуждение того или иного вопроса, а телефонный аппарат установлен так, что его индикаторы не видны присутствующим.

Угроза наличия недокументированных возможностей.

Недокументированные возможности самих аппаратов (в особенности IP-) являются еще одной угрозой для конфиденциальности речевой информации в защищаемых помещениях. Программное обеспечение IP-телефонов представляет собой сложный программный комплекс, в т.ч. реализующий стек протоколов TCP/IP, и может содержать:

- недокументированные возможности, внесенные разработчиками в целях тестирования или на определенных этапах разработки новых функциональных возможностей аппаратов;

- ошибки в реализации, например, приводящие к уязвимостям класса «переполнение буфера», и позволяющие получить полный контроль над программным обеспечением аппарата до его перезагрузки.

Примером угрозы первой группы является имевшаяся в одной из версии ПО возможность отправки на IP-телефоны наиболее популярных моделей 7940 и 7960 компании Cisco Systems Inc. управляющего XML-сообщения CiscoIPPhoneExecute, которое среди прочих возможностей (набор номера, эмуляция нажатия клавиш и т.п.) могло включать микрофон аппарата и передавать весь голосовой трафик на указанный в XML-сообщении IP-адрес.

Угроза прослушивания IP-трафика в момент передачи по сети.

Различные варианты реализаций угроз прослушивания трафика традиционны для компьютерных сетей, использующих в своей структуре широковещательные сегменты (Ethernet, в т.ч. коммутируемый, радио-Ethernet и т.п.), и создают еще один уровень возможных атак на системы IP-телефонии. При отсутствии шифрования трафика на сетевом или более высоких уровнях модели OSI существует несколько вариантов нарушения конфиденциальности передаваемых сообщений.

В условиях отсутствия у злоумышленника административных прав на активное сетевое оборудование наиболее эффективной в коммутируемых Ethernet-сетях является атака «ARP spoofing», выполняющая изменение таблицы маршрутизации на канальном (MAC) уровне с помощью специально сформированных ARP-пакетов. Также к раскрытию определенной части передаваемой информации может привести перевод коммутатора в режим концентратора с помощью большого количества фальшивых пакетов (MAC storm), хотя этот способ и обладает значительными демаскирующими признаками, выражающимися в резком снижении качества работы сети.

При получении злоумышленником административных прав на коммутирующем или маршрутизирующем оборудовании (например, в результате атаки на компьютер администратора или при перехвате его пароля, передавшегося в открытом виде) у него появляются гораздо более мощные средства перехвата IP-трафика. Они включают:

- возможность активации на коммутаторах зеркальных (SPAN) портов, получающих точную копию передаваемого по определенным портам трафика;
- использование иных технологий «ответвления» трафика от производителей сетевого оборудования, например:
  - протокола ERSPAN (Encapsulated Remote SPAN), инкапсулирующего каждый перехватываемый пакет в пакет протокола

GRE, что позволяет передавать его по IP-сетям без каких-либо ограничений дальности;

– опции IP Traffic Export, реализующей "ответвление" трафика при его маршрутизации на 3-ем уровне модели OSI;

Оба протокола поддерживают возможность тонкой настройки фильтрации перехватываемых пакетов, что позволяет копировать трафик только от определенных групп IP-устройств.

Беспроводные сети при отсутствии стойких алгоритмов шифрования также являются потенциальным источником раскрытия передаваемого по ним голосового трафика.

Угроза подмены сообщений в управляющем канале.

Методика централизованного управления IP-телефонными вызовами (реализуемая в УАТС) содержит еще один возможный путь прозрачного для абонентов перехвата их разговоров. В момент установления IP-соединения первоначальный обмен информацией, содержащей номера абонентов, их имена, технические возможности аппаратов и т.п., в т.ч. IP-адреса оконечных устройств, идет между серверами IP-телефонии. На этом этапе возможна подмена (средствами атак сетевого уровня) информации об одном или обоих IP-адресах с целью внедрения противника в цепочку передачи голосового трафика по принципу прозрачного прокси-сервера.

Подобный класс атак остается совершенно незаметным на прикладном уровне, т.к. пользователю обычно не видны сетевые координаты удаленного абонента, а стек протоколов не способен обнаружить факт подмены, и может быть выявлен только с помощью специализированного мониторинга сетевого трафика.

В целом, предпосылкой для появления возможности подобных атак является то, что в современных протоколах IP-телефонии (H.323, SCCP и др.) оконечное оборудование при приеме и передаче голосового потока является ведомым относительно сервера УАТС и полностью полагается на информацию, сообщенную ему в управляющем канале (в т.ч., например, не проверяет соответствие IP-адресов отправителя и получателя голосового потока в рамках одного и того же разговора). Проблема обеспечения защиты от внедрения в голосовой поток прокси-сервера поднимает вопрос об обеспечении целостности передаваемых в управляющем канале данных стойкими криптографическими методами.

4. Заключение. Анализ результатов поисковых исследований DAPRA [3] свидетельствует о появлении и необходимости нейтрализации новых угроз кибербезопасности. Известные публикации газеты «The Washington Post» на основе заявлений Э.Сноудена подтверждают

реализацию упомянутых киберугроз на практике. Разведслужбы США в течение только 2011 года провели против других стран 231 кибератаку, были потрачены более 652 мл. долларов США. При этом три четверти кибератак были направлены против России, Ирана, Китая и Северной Кореи, в т.ч. ядерные программы этих стран. По мнению Э. Сноудена США провели более 61 тысячи хакерских кибератак по всему миру. Все вместе это подтверждает актуальность постановки и проведения специальных НИОКР по своевременному выявлению и парированию выявленных киберугроз цифровой обработки данных.

Литература

1. *Клабуков И.Д., Алехин М.Д., Нехина А.А.* Исследовательская программа DARPA на 2015 год // М. 2013. 102 с.
2. *Клабуков И.Д., Алехин М.Д., Мусиенко С.В.* Сумма технологий национальной безопасности и развития // М. 2013. 110 с.
3. Официальный сайт агентства по перспективным оборонным научно-исследовательским разработкам Defense Advanced Research Projects Agency, DARPA. URL: www.darpa.mil (дата обращения: 12.01.2015).
4. *Kellerman T.* Cyber-threat proliferation: Today's truly pervasive global epidemic // Security Privacy, IEEE. 2010. vol. 8. no. 3. pp. 70–73.
5. *Wilshusen G.C.* Cyber threats and vulnerabilities place federal systems at risk: Testimony before the subcommittee on government management, organization and procurement // United States Government Accountability Office. Tech. Rep. 2009.
6. *Musliner D.J., Rye J.M., Thomsen D., McDonald D.D., Burstein M.H.* FUZZBUSTER: Towards adaptive immunity from cyber threats // In 1st Awareness Workshop at the Fifth IEEE International Conference on Self-Adaptive and Self-Organizing Systems. 2011. pp. 137–140.
7. *Musliner D.J., Rye J.M., Marble T.* Using concolic testing to refine vulnerability profiles in FUZZBUSTER // In SASO-12: Adaptive Host and Network Security Workshop at the Sixth IEEE International Conference on Self-Adaptive and Self-Organizing Systems. 2012. pp. 9–14.
8. *Musliner D.J., Friedman S.E., Rye J.M., Marble T.* Meta-control for adaptive cybersecurity in FUZZBUSTER // Proc. of 7th IEEE Int. Conf. on Self-Adaptive and Self-Organizing Systems. 2013. pp. 219–226.
9. *Burnim J., Sen K.* Heuristics for scalable dynamic test generation // Proceedings of the 23rd IEEE/ACM International Conference on Automated Software Engineering, ser. ASE '08. 2008, pp. 443–446. URL: http://dx.doi.org/10.1109/ASE.2008.69.
10. *Weimer W., Forrest S., Goues C.Le, Nguyen T.* Automatic program repair with evolutionary computation // Communications of the ACM. 2010. vol. 53. no. 5. pp. 109–116.

References

1. Klabukov I.D., Alehin M.D., Nehina A.A. *Issledovatel'skaja programma DARPA na 2015 god* [DARPA research program for 2015]. M. 2013. 102 p. (In Russ.).
2. Klabukov I.D., Alehin M.D., Nehina A.A. *Summa tehnologij nacional'noj bezopasnosti i razvitija* [Sum of technologies to national security and development]. M. 2013. 110 p. (In Russ.).

3. Oficial'nyj sajt agentstva po perspektivnym oboronnym nauchno-issledovatel'skim razrabotkam [Official web site of Defense Advanced Research Projects Agency, DARPA]. Available at: www.darpa.mil. (accessed 12.01.2015).
4. Kellerman T. Cyber-threat proliferation: Today's truly pervasive global epidemic. *Security Privacy, IEEE*. 2010. vol. 8. no. 3. pp. 70–73.
5. Wilshusen G.C. Cyber threats and vulnerabilities place federal systems at risk: Testimony before the subcommittee on government management, organization and procurement. United States Government Accountability Office. Tech. Rep. 2009.
6. Musliner D.J., Rye J.M., Thomsen D., McDonald D.D., Burstein M.H. FUZZBUSTER: Towards adaptive immunity from cyber threats. In 1st Awareness Workshop at the Fifth IEEE International Conference on Self-Adaptive and Self-Organizing Systems. 2011. pp. 137–140.
7. Musliner D.J., Rye J.M., Marble T. Using concolic testing to refine vulnerability profiles in FUZZBUSTER. In SASO-12: Adaptive Host and Network Security Workshop at the Sixth IEEE International Conference on Self-Adaptive and Self-Organizing Systems. 2012. pp. 9–14.
8. Musliner D.J., Friedman S.E., Rye J.M., Marble T. Meta-control for adaptive cybersecurity in FUZZBUSTER. Proc. of 7th IEEE Int. Conf. on Self-Adaptive and Self-Organizing Systems. 2013. pp. 219–226.
9. Burnim J., Sen K. Heuristics for scalable dynamic test generation. Proceedings of the 23rd IEEE/ACM International Conference on Automated Software Engineering, ser. ASE '08. 2008, pp. 443–446. URL: http://dx.doi.org/10.1109/ASE.2008.69.
10. Weimer W., Forrest S., Goues C.Le, Nguyen T. Automatic program repair with evolutionary computation. Communications of the ACM. 2010. vol. 53. no. 5. pp. 109–116.

Петренко Сергей Анатольевич — д-р техн. наук, директор, Центр систем кибербезопасности АФК "Система", научный эксперт Совета Безопасности РФ. Область научных интересов: компьютерные науки, кибербезопасность, программирование. Число научных публикаций — 80. s.petrenko@rambler.ru, http://www.htsts.ru; Б. Грузинская, д. 12, стр. 2, Москва, 123242; р.т.: +79037428543, Факс: +79037428543.

Petrenko Sergei Anatol'evich — Ph.D., Dr. Sci., director, Center for Systems Cybersecurity AFK "Sistema", scientific expert of the Security Council of the Russian Federation. Research interests: computation with memory, cybersecurity, theoretical programming. The number of publications — 80. s.petrenko@rambler.ru, http://www.htsts.ru; 12, Bolshaya Gruzinskaja, Building 2, Moscow, 123242; office phone: +79037428543, Fax: +79037428543.

РЕФЕРАТ

Петренко С.А. **Модель киберугроз по аналитике инноваций DARPA.**

В работе проведен анализ современных поисковых исследований агенства DARPA в области кибербезопасности. Определена новая модель киберугроз цифровой обработки данных. Здесь под киберугрозами понимаются действия или события, которые могут привести к нарушению способности выполнения основных целевых задач объекта информатизации. По характеру проявления киберугрозы разделены на преднамеренные (умышленные) и непреднамеренные (случайные). Косвенные киберугрозы связаны с попытками несанкционированного доступа к информации без физического доступа к элементам системы, а прямые – с попытками несанкционированного доступа к информации с физическим доступом к элементам системы. В зависимости от используемых методов реализации киберугрозы разделены на пассивные и активные. Пассивные киберугрозы имеют целью несанкционированный доступ к информации без изменения состояния информационной системы. Примером пассивной угрозы может служить перехват передаваемой по каналам и линиям связи информации для последующего ее анализа. Активные киберугрозы имеют целью намеренное несанкционированное изменение состояния, например, хищение или модификации конфиденциальной информации. В качестве источника активных угроз могут также выступать специальные средства, называемые закладками (программными, аппаратными или программно-аппаратными), компьютерные вирусы, вредоносное программное обеспечение, которые могут быть встроены в программно-аппаратные средства информационных систем на этапе их изготовления, или внедрены в них в процессе эксплуатации.

Подробно рассмотрены следующие киберугрозы цифровой обработки данных: подключение к каналам связи, прослушивание разговоров в помещении с помощью автоответа, наличие недокументированных возможностей, прослушивание IP-трафика в момент передачи по сети, подмена сообщений в управляющем канале. Определена соответствующая модель киберугроз цифровой обработки данных и предложены рекомендации по своевременной нейтрализации упомянутых киберугроз.

SUMMARY

Petrenko S.A. **Model Cyber Threats by Analysis of DARPA Innovations.**

The analysis of modern exploratory research of agency DARPA in cybersecurity was carried out. A new model of cyber digital data processing is defined. Here the activities under cyber threats or events that may disrupt the ability to perform the basic targets of the object information are analyzed. Cyberthreats by the nature of manifestations are divided into intentional (deliberate) and unintentional (accidental). Indirect cyber threats are associated with unauthorized access to information without having physical access to the elements of the system, and direct - to attempt to gain unauthorized access to information with physical access to the system elements. Depending on the used methods of implementing cyberthreats divided into passive and active. Passive cyberthreats aim to unauthorized access to the information without changing the state of the information system. An example of a passive threat can serve the intercept of transmitted channels and lines of communication of information for its subsequent analysis. Active cyberthreats aim intentional unauthorized changes to the state, such as theft or modification of sensitive information. As a source of active threats may be also special tools called tabs (software, hardware, or software and hardware), computer viruses, malicious software, which can be embedded in software and hardware information systems at the stage of manufacture, or embedded in them during operation.

Discussed in detail the following cyberthreats for digital data processing: connection to communication channels, listening to conversations in the room with the help of auto-answer, the presence of undocumented features, listening to IP-traffic at the time of transmission over the network, the substitution of messages in the control channel. The appropriate model cyberthreats of digital data and recommendations on timely neutralizing mentioned cyberthreats are determined.